TOWARDS THE DEVELOPMENT OF A DEFENSIVE CYBER DAMAGE AND MISSION IMPACT METHODOLOGY

THESIS

Larry W. Fortson, Jr., Captain, USAF

AFIT/GIR/ENV/07-M9

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/07-M9

TOWARDS THE DEVELOPMENT OF A DEFENSIVE CYBER DAMAGE AND MISSION IMPACT METHODOLOGY

THESIS

Presented to the Faculty

Department of Systems Engineering and Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Larry W. Fortson, Jr., BS

Captain, USAF

March 2007

AFIT/GIR/ENV/07-M9

TOWARDS THE DEVELOPMENT OF A DEFENSIVE CYBER DAMAGE AND MISSION IMPACT METHODOLOGY

Larry W. Fortson, Jr., BS
Captain, USAF

Approved:

//SIGNED//	16 Mar 07
Michael R. Grimaila, PhD, CISM, CISSP (Chairman)	date
//SIGNED//	16 Mar 07
Robert F. Mills, PhD (Member)	date
//SIGNED//	16 Mar 07
Dennis D. Strouble, PhD (Member)	date
//SIGNED//	16 Mar 07
David A. Van Veldhuizen, Lt.Col., USAF, PhD (Member)	date
//SIGNED//	16 Mar 07
Lisa S. Thiem, Captain, USAF (Member)	date

Abstract

The purpose of this research is to establish a conceptual methodological framework that will facilitate effective cyber damage and mission impact assessment and reporting following a cyber-based information incidents. Joint and service guidance requires mission impact reporting, but current efforts to implement such reporting have proven ineffective. This research seeks to understand the impediments existing in the current implementation and to propose an improved methodology. The research employed a hybrid historical analysis and case study methodology for data collection through extensive literature review, examination of existing case study research and interviews with Air Force members and civilian personnel employed as experts in cyber damage and mission impact assessment of Air Force networks. Nine respondents provided valuable first hand information about the current implementation cyber damage and mission impact assessment. This research identified several critical impediments to current mission impact assessment efforts on Air Force networks. Based upon these findings, a proposal is made for a new operations-focused defensive cyber damage and mission impact methodology. The methodology will address the critical impediments identified and will result in profound benefits in other areas of cyber asset protection. Recommendations for conceptual implementation and operationalization are presented and related future research topics are discussed.

Acknowledgements

I would like to express my sincere thanks to several people to whom I am greatly indebted for their patience and assistance in this thesis effort. First, I thank AFRL/HEX, whose sponsorship made this research possible. Secondly, I would like to thank my advisor and thesis committee chair, Dr. Michael Grimaila. His guidance and patience was invaluable to the completion of this research. I would also like to express my profound appreciation to the 33rd Information Operations Squadron, Lackland AFB, whose men and women tirelessly keep the bad actors out of Air Force networks. My most sincere thanks also go to the Air Force Network Operations Center Network Control Division and the Air Force Information Operations Center, whose interest and assistance in the continuation of this research effort is greatly appreciated.

I would especially like to thank my wife and son for their unending patience and support through this research effort. Simple words cannot express my gratitude.

Table of Contents

Page

Page

Page

List of Figures

Page

List of Tables

TOWARDS THE DEVELOPMENT OF A DEFENSIVE CYBER DAMAGE AND MISSION IMPACT METHODOLOGY

I. Introduction

> *"Success in the twenty-first century battlespace will rely more and more on our ability to use and protect information. Quality information is the counter to the fog of war. Military operations make special demands on information functions and we must meet those demands if we are to give our commanders the information advantage. Information superiority is just like air superiority or space superiority: it gives us the freedom and ability to operate in the information domain while denying it to the enemy."* Statement of Lt. General Donahue before the House Military Procurement and Research and Development Subcommittee (1997)

Background

The past several decades have been witness to a revolution information technology (IT). This revolution has resulted in an ever-growing reliance upon IT in developed and developing nations. Networking technology, and the Internet in particular, has given both business and government organizations alike the promises of greater efficiency through networked computing. The IT boom of the 1980s and 1990s produced a dependence on digital information assets making internal and external networks central to the modern organization's information infrastructure. In a relatively short time, cyber-based digital information became a critical asset on which the operational and strategic operations of the modern enterprise depend (Denning 1999, pp. 13-15). Information has become a transnational commodity and every modern business organization has become an information organization (Drucker 1993, pp. 89, 143-145).

The Department of Defense (DoD) was quick to recognize the potential benefits of automating processes with IT and readily embraced the new technologies. Today the

daily operations of the virtually every United States government agency maintain a great dependency on IT and the light-speed exchange of information in cyber space. This is especially true of the armed services when this dependence upon cyber information was first notably demonstrated during the Persian Gulf War; the first war where cyber technologies were used to great effect in support of combat actions in the air, ground, and sea (Gumahad 1997). Organizations whose critical mission processes maintain such a great dependence on cyber information result in an environment where information compromise, damage, loss can equate to mission failure (Kemmerer 2003, p. 705). This makes the need to protect and defend information assets in cyberspace a paramount requirement to ensure the organization's success (GAO 2005). Inevitably, such organizations are forced to deal with an information incident, whether by malicious intent, accident, or natural disaster. When this happens, the organization's decision maker must have a timely and clear picture of how the incident as impacted the organization's ability to accomplish its mission. Success in military operations depends on providing the commander rapid and accurate battlespace awareness. Part of this is gaining an understanding how cyber incidents affect the organization's ability to accomplish the mission.

The Need for a Defensive Cyber Damage Assessment Framework

Since the beginning of organized warfare, commanders have attempted to assess the impact of offensive actions against the enemy's war fighting assets (Diehl and Sloan 2005, p. 59), as well as understand the impact of a successful enemy attack against friendly warfighting assets. As the DoD continues to integrate kinetic operations into

cyber space, the more valuable asset information becomes. Annual surveys conducted by the Federal Bureau of Investigations (FBI) determined that the reported economic losses from cyber security incidents continued a four-year decline in 2006 (Gordon 2006, p. 12). This is a possible indicator that these organizations are more secure. It could be, however, that economic metrics are not accurately portraying the extent of damage that these organizations are truly experiencing from the cyber incidents. Despite the best of efforts to prevent such security breaches, many attacks against cyber information assets successfully breach network defenses. This is extremely worrisome for organizational decision makers who understand that the continued growth in successful attacks, coupled with the ever-growing dependency of kinetic operations upon cyber assets, creates an environment for unprecedented 'hidden' damage to warfighting capabilities. In 2004, Department of Defense officials acknowledged that these successful intrusions had resulted in reduced military operational capability (Tiboni 2005b).

Commanders are now beginning to ask the hard questions of 'how' a cyber attack affects both their respective organization and the mission operations as a whole. In fact, recently amended military joint guidance (CJCSM6510.01 2006) requires commanders to ensure operational impact assessment is accomplished following a network incident. In the cyber realm, however, DoD organizations are finding it difficult to accurately map damage assessment to operational impact after an information compromise occurs.

In 1996, the Department of Defense (DODD5220.22-M) conducted a series of "day after" games to measure their ability to effectively respond to cyber attacks. These exercises demonstrated that the DoD was not ready to respond effectively to such attacks. A report following these exercises cited four critical issues that must be addressed to

improve the DoD's ability to respond to these cyber attacks if they were to happen in the real world. Among these was the need for "a 'battle damage' assessment process suitable for IW" (Alberts 1996, pp. 24-25). Ten years later, there still exists no standardized operational damage assessment model for information compromises on United States Air Force (USAF) networks (Thiem 2005).

Despite the need to understand the organizational impact caused by information incidents, surprising little research has focused in this area (Horony 1999). The work that does exist tends to be funded by the private, for-profit sector and to focus providing awareness for decision making on the financial impact the organization. The models established by these works yield economic metrics. Economic measurements are more tangible than other forms of impact metrics (Horony 1999) and lend themselves more easily to complex calculation in damage models that attempt to quantify an incident's financial cost to the organization. Indeed, these models meet the decision-making needs of many for-profit, private sector organizations. Nevertheless, such models and metrics are far less useful to those organizations with missions not economically driven; such as those that exist within the DoD and other critical branches of government. In these areas, and especially in the context of military operations, the financial value of information is of very low importance. Economic metrics simply do not provide commanders with the information necessary to make smart and timely decisions after an information compromise.

To illustrate this point, consider the following real world example illustrating how cyber attacks on information assets can directly impact a military organization's physical mission. In early 2004, network defenders watching for suspicious activity on networks

supporting Multinational Force-Iraqi (MMF-I), at that time called the Combined Joint Task Force Seven, were reporting as many as 60 new computer network incidents each day. With network control locations dispersed widely across the Iraq theater of operations, and no defensive damage assessment framework in place to predicatively assess potential impact to the mission in event of a successful cyber incident, computer incident response was extremely difficult. In all cases, it was a "wait and see" activity to determine the extent of damage to both network operations and the ripple effect of impact to mission operations. Damage assessment consisted of solely post-recovery analysis that *reported* the impact to mission capability long after the fact rather than assessed the impact in a timely manner. No framework existed that allowed local information owners or custodians to both identify the information assets stored on potentially compromised systems and work with incident responders to assess damage to the overall mission. This left many forward deployed units with limited and occasionally no access to important information stored on military servers at *the rear*. This problem was compounded by a poor, disjointed framework for incident reporting, which in at least one case contributed to human casualties.

There is a dire need for an efficient framework to assess the impact to an organization's information assets and provide the decision maker with an understanding of the impact to the organization's mission capability following a compromise. By providing the commander with a timely and clear sight picture of any degradation to their own mission capability, the commander is better prepared to make better decisions in accomplishing the mission.

Problem Statement

Defensive cyber damage assessment metrics produced by damage assessment methodologies currently employed on Air Force networks do not enable commanders to see the *mission capability* impact resulting from a cyber compromise. Nearly all existing methodologies assess the economic impact of a cyberspace incident. While economic impact can be a factor a commander may consider when justifying IT and security upgrades, it is of little value as a decision input factor in military operations. Attempts to assess damage following a compromise of Air Force networks have been less than successful for a wide range of reasons and the chief of these may lie in the Air Force's fundamental approach and perspective regarding network security.

The Air Force approaches cyber security from an infrastructure-focused perspective. This approach focuses on protecting the organization's IT infrastructure against known technological vulnerability-focused scenarios. According to Soo Hoo (2005) this approach is inherently limited in its ability to identify the risks to the assets the organization means to protect (Soo Hoo 2000, p.11). Vulnerability is only significant if it places a critical *asset* at risk (Stevens 2005, p. 14). Rather than identifying the information assets within the system and determining the relative value they present to the organization organizational mission, this approach explicitly focuses on technical components of infrastructure technological assets. This approach overlooks information and substitutes its value to the organization with that of the infrastructure components and cannot account the value of the organization's most important asset—its information. The assumption that technology is an equitable substitute for information is a dangerous assumption and follows a proven path of failure (Davenport and Prusack 1998).

The DoD is beginning to realize that this approach imposes inherent limitations on attempts attempting to perform damage assessment. When an information incident occurs, the agency responsible for incident response activities must conduct a mission impact assessment to quantify the value of the affected information asset contributes to the organization's mission. This is especially true in DoD agencies where the incident response agent exists outside the organization. In nearly all cases, no documentation of information asset value exists to aid the incident response agent in understanding its value. As a result, subsequent efforts to identify and quantify the impact are subjective and unreliable, and produce little or no usable for use in timely and reliable decision-making.

There is currently no effective methodology to assess the damage to information assets on Air Force networks, estimate the impact to organizational mission, and effectively report timely and accurate impact assessment to decision makers following a cyber security incident on Air Force Networks.

Problem Approach

The shortcomings in the current approach to damage assessment are evident in the failure to provide organizational decision makers with an understanding of how a cyber incident affects the organization's mission. Several issues may contribute to this problem. This research will approach the problem with an examination of how the Air Force implements damage assessment and what issues may be impeding effective damage and mission impact assessment efforts. The research will attempt to understand how the Air Force identifies and values its cyber assets, since understanding the value of

the organization's critical cyber-based information assets is fundamental to determining the extent of damage and subsequent mission impact following a cyber attack.

To this end, this research must discover what obstacles may be preventing cyber damage and mission impact assessment, as well as what issues may be contributing to these efforts. Successful and accurate cyber damage and mission impact assessment depends on the successful and effective accomplishment of a number of supporting activities. Such key supporting activities are identification of the correct cyber assets in an organization, determining their relative value to the organization, determining damage after an incident, and mapping that damage to an effect on the organization's mission. Damage assessment is only the first step and mission impact assessment should be the ultimate goal of cyber damage assessment on military networks.

Ultimately, this research will propose an ideal methodology for defensive cyber damage and mission impact assessment to allow organizations to understand how a successful cyber incident affects its mission.

Research Questions

This research aims to answer three questions that are essential to the development of a Defensive Cyber Damage Assessment framework:

> *R1. How can the damage resulting from a successful cyber attack be effectively measured in a non-profit driven organization?*
>
> *R2. How can such damage be mapped to impact to an organization's mission capability?*
>
> *R3. How must this assessment be reported to the decision maker to maximize the quality of the assessment for use as decision input?*

To effectively answer these questions, this research aims to determine how damage is currently being assessed, how to what degree impact to mission operations is assessed, and what, if any problems exist in the current methodology.

Foundational Terminology

Defining a canonical terminology is essential when communicating ideas to diverse communities of interest. For this reason, we now define the terminology used in the Defensive Cyber Damage and Mission Assessment (CDA-D/MIA) framework proposed in this paper. First, the scope and purpose of defensive cyber damage assessment must be established. Joint Publication 1-02 defines military damage assessment as "an appraisal of the effects of an attack on a nation's military forces to determine residual military capability and to support planning for recovery and reconstitution" (JP 1-02 2006, p. 336). Historically, the focus of damage assessment has been on the effects of offensive actions against the mission capability of enemy forces. Conversely, our work is focused upon defensive damage assessment which appraises the effects of a cyber-based incident that potentially impacts friendly mission capability. For the purposes of our research, a *mission* describes the overall purpose of the organization. The term mission is also used in a similar context to define the goals and objectives of a specific department, group, or unit within the organization. Thus, the overall mission of an organization is comprised of a hierarchy of subordinate missions, with an over-arching enterprise mission being supported by the missions of its organizations. Each organization may have supporting departmental missions. This hierarchy is an "essential component of operational effectiveness" (Alberts and Dorofee 2005, p.4).

A mission is supported by one or more operational processes as shown in Figure 1 below. Operational processes are those processes that enable people or systems to accomplish the mission. In modern organizations, most operational processes are supported by one or more information processes. Information processes are those information flows that support the operational process. An organization's information processes depend on information assets. An information asset is a set of information that holds value to the organization's mission. A cyber information asset is information that resides electronically within cyberspace. A cyber information asset may be information stored on the organization's server infrastructure or an information flow on which the organization depends. A *critical* cyber information asset is one which the organization depends upon to accomplish its tactical, operational, or strategic mission. *Damage* is defined as a reduction in value or usefulness of the object affected (Oxford, 1986). Damage or loss of a critical cyber information asset potentially would result in impairment of the organization's mission. This impairment to the organization's mission is called *impact*. Damage and impact are related, but are not the same. Impact is generally the result of some damage. Since this research deals explicitly with defensive damage assessment of cyber-based assets, all references to information assets imply cyber information assets.

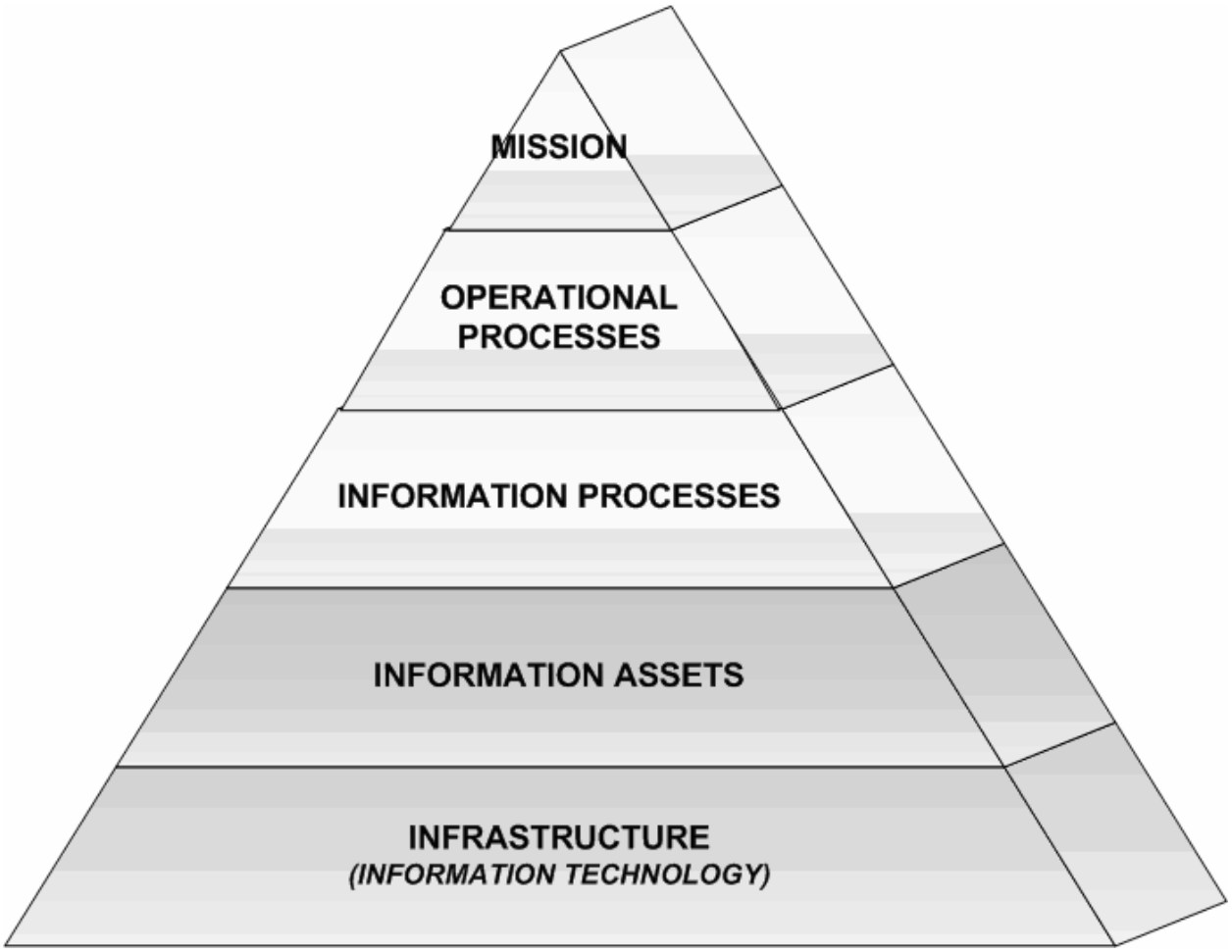


Figure 1. Mission Structure Hierarchy

Most traditional approaches to damage assessment make no difference between data and information. However, some very distinct and important differences between data and information exist. Data is the elemental subset of information that possesses no inherent value, but is dependent on external application. This external application assigns value to the information. Information is aggregation of data that is grouped in such a way that meaning and value are both inherent and vary contextually (Petrocelli 2005, pp. 180-181). This important characteristic of information is fundamental to developing a foundation on which to build effective cyber damage assessment. All information assets

have producers, owners, consumers, and custodians. The information producer is the creator of the information or the originator of an information flow. The information owner is the entity that bears responsibility for determining the classification, value, and level of protection of the information asset commensurate with its value. The information custodian is the entity responsible for implementing the security measures that protect the information asset. An information consumer is any entity that maintains transitive dependencies on the information. It is important to understand that the information producer, owner, custodian, and consumer are all closely related; and they can be the same entity.

Research Scope

Defensive cyber damage assessment methodology is an important part of gaining a heightened level of mission assurance in any organization reliant on cyber-based information. The overall perspective of this thesis research, however, is from a military operations perspective. This research aims to develop a defensive cyber damage and mission impact assessment framework to provide decision makers, the commanders, situational awareness of how a cyber information compromise affects his/her mission capability through understanding the value of the critical information assets on which the mission relies. This is primarily concerned with aiding the commander working in the tactical and operational domains of operations. The framework intends to provide useful metrics for decision makers operating in the strategic domain of operations.

This research recognizes that different communities of interest in both the public and private sector have specific requirements and expectations for a damage assessment

model. It is also important to note there are varying assumptions of the methodology and scope of a defensive introduced by the widely varying experiential perspectives of the communities of interest that may desire to implement such a framework. For example, the network security community of interest may feel strongly that the commander must know how and why an intruder was able to gain access to and compromise critical assets on the network. These activities are extremely important and are accomplished by the agencies tasked with that responsibility. This type of information, while important in preventing future malicious incidents, it may not be useful to the commander who needs to know how the incident has affected his immediate mission operations. Development of a mission impact assessment methodology for organizations not driven by economic profit is the goal of this research. For this reason, the scope of research is different from existing models that attempt to assign value as an economic function. This research will attempt to discover a new way to determine cyber asset value in terms that are meaningful to an organization that is not driven by economic gain. By determining asset value, the research intends to determine a damage assessment methodology that allows mapping between the asset and the mission operations that the asset supports.

Thesis Structure

This research employs qualitative research methods in order to answer the research questions. The quest for answers to the research questions presented in this chapter require a multiple vectored approach to gathering appropriate data. This chapter presents and introduction to the material, but Chapter 2 delves into an extensive literature review of the large information space that is required to develop a sound understanding of damage and mission impact assessment.

Chapter 3 presents a detailed discussion of the research methodology. In order to understand the methods and problems with current damage assessment methodology and mission impact estimation techniques currently being used on the Air Force networks, this research depends on existing research and interviews with agencies involved with Air Force network operations and network defense activities.

Chapter 4 discusses, analyses, and synthesizes the data collected through the extensive literature review, examination of existing case study research, and interviews performed in this research effort. Chapter 4 will present the findings of this research as they relate to the investigative research question presented in Chapter 1.

Chapter 5 presents a conclusive proposal for an improved cyber damage and mission impact assessment model. The proposed Defensive Cyber Damage and Mission Impact Assessment methodology is a comprehensive methodology that if properly implemented would correct the weaknesses in the current approach that results in unsatisfactory impact awareness on Air Force networks.

Research Limitations

The DoD has been admittedly slow to address the area of defensive cyber damage assessment and as a result this is still a relatively immature area of research. The DoD maintains a highly segmented structure and this research effort proceeds forward with the understanding that there may be related work underway in other segments of the DoD to address this issue. In an effort to present this work in an unclassified format, some issues will not be addressed to prevent potential disclosure of sensitive information; particularly those involving specifics of network offensive activities, network defense specifications and procedures. However, this framework will maintain a generic quality to allow

application in these areas not explicitly addressed in this work. Additionally, since the focus of this research effort is development of a defensive cyber damage assessment for military networks, the specific audience is limited to those potential users to do not utilize financial loss as a driver for decision making.

Another limitation is the absence of data to demonstrate the degree of effectiveness in a practical sense, and validity in an academic sense of this research. It is hoped that future research will address these issues.

II. Literature Review

Introduction

> "Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. (Sun-Tzu 1993)"

The information revolution changed the face of the modern organization. In both government and private sector alike, the new technology of this revolution created new ways for information to flow through and within an organization. These changes both flattened traditional decision-making hierarchies and forced a massive re-engineering of the way business is done (Drucker 1993, pp. 89). Every organization that maintains reliance upon information cyberspace is in the information business. For this reason, virtually every modern organization is an information organization (Drucker 1995). This includes the military.

The advent of cyberspace was a dual edged sword. It offered great promises of efficient production and reduced operating costs, but also introduced new and unexpected risks and vulnerabilities. Organizations embraced the promises of cyberspace technology without thought for security; and many quickly found themselves ill prepared for these new problems. Recent years have witnessed many private sector and government organizations fall victim to malicious activity, mishap, and natural disaster that has degraded or removed access to cyber information with grave impact to the organization's ability to conduct normal mission operations. Literature review shows that despite the evolution towards stronger security, vulnerabilities and successful exploits maintain and annual increase (CERT 2006). Since "perfect security is not attainable" (Mimoso 2005),

organizations must be prepared to efficiently handle the impact of a successful attack. An organization must also be able to understand how the incident impacts the organization's *mission capability.* Mission capability refers to the organization's ability to accomplish its tactical, operational, and strategic business goals. Exhaustive literature review has demonstrated that relatively little research has been conducted on mission impact following a cyber attack. With only a few exceptions, research in this area is limited to determination of the economic costs associated with remediation and recovery from a cyber incident. As cyber warfare continues to evolve, many organizations that are not profit driven, such as military organizations, are discovering that cost loss does not provide the right input information for smart and timely operational decisions after being hit. This literature review explores the essential concepts of cyberwarfare, information value, and other concept critical to the foundations of a defensive cyber damage assessment framework.

Cyberwarfare and Defensive Damage Assessment

Information is the center of gravity of cyberspace. The ever-growing American dependence on cyberspace has made information a critical center of gravity on which national security depends (Billo and Chang 2004, p. 22). Denning identifies information as a valued asset to both owner and adversary; therefore, it is an asset that must be protected (Denning 1999, pp. 22-25). President George Bush accurately noted, however, "…there is no such thing as perfect security. (Bush 2004) "; and his words hold particularly true in the cyber domain. The DoD has recognized that successful attacks against cyber information inevitably occur and when such attacks successfully damage

the organization's information assets real world mission operations can be affected (Tiboni 2005b).

When an attack is successful, it is essential to perform immediate incident response to arrest propagation of the incident as quickly as possible. Additionally these incident response actions are part of damage assessment activities that help the organization understand the impact and make the right decisions for recovery and mission operations (Lala and Panda 2000, p. 300). Mission success can, and often does, depend on a clear understanding of how the cyber attack has degraded the actual or potential capabilities of kinetic mission operations. This section will examine literature discussing the nature of cyber space and cyber warfare, briefly examine the evolution of military operational dependence upon cyber space, and the importance of defensive cyber damage assessment to ensuring successful military operations in both cyberspace and the real world.

What is cyberspace?

Understanding the cyber battlespace if fundamental to understanding cyber warfare. The concept of cyberspace was originally conceived by science fiction author, William Gibson (1984) to describe a virtual and alternate world that existed in the electronic space between every computer in the human system. In Gibson's vision, virtual *cyberspace* was a virtual domain of virtual dimension and space that imitated the modern world, the *realspace* of the human world. Cyberspace and realspace are integrated such that the effect of activities in one domain could affect the other. The American Heritage New Dictionary of Cultural Literacy, 3d Edition, defines cyberspace in the following way:

> "The space in which computer transactions occur, particularly transactions between different computers. We say that images and text on the Internet exist in cyberspace, for example. The term is also often used in conjunction with virtual reality, designating the imaginary place where virtual objects exist. For example, if a computer produces a picture of a building that allows the architect to [*walk*] through and see what a design would look like, the building is said to exist in cyberspace. (American Heritage n.d.)"

In many ways, Gibson's predictive definition of the cyber realm has become something close to a reality. Joint Publication 1-02 concisely defines cyberspace as "the notional environment in which digitized information is communicated across computer networks (JP 1-02 2006, p. 139)." The Internet is often considered to *be* cyberspace, but it is actually only a part of it. Cyberspace is that place between all computers—a massive exchange of information at light speed between "the sum total of all computer networks (Denning 1999, p. 22)."

The United States government has realized that physical assets are vulnerable to attacks from cyberspace. As Department of Homeland Security Secretary Tom Ridge stated,

> "Cyber security cuts across all aspects of critical infrastructure protection. Most businesses in this country are unable to segregate the cyber operations from the physical aspects of their business because they operate interdependently (USCERT 2003)"

Many security experts have expressed concern that America's ever-growing dependence on cyberspace has become its Achilles heel (Blodgett 1999).

What is cyber warfare?

The term cyber warfare is often confused with information warfare. Denning describes information warfare as consisting "of offensive and defensive operations against information resources of a 'win-lose' nature. It is conducted because information

resources have value to people (Denning 1999, 67)." Cyber warfare, itself, may be loosely viewed as that part of information warfare that occurs within the domain of cyberspace; and uses the technologies of that realm. Cyberwarfare activities are part of the many constructs of Information Operations. (IO). IO covers broad spectrum of activities and therefore overlaps the boundaries of many different communities of interest. As a result, different communities maintain slightly differing perspectives of what cyber war is in relations to their respective interest.

In 1993, John Arquilla and David Ronfeldt introduced the concept of cyberwarfare to describe knowledge-centric conflict in military operations. They describe cyberwar in this way:

> "Cyberwar refers to conducting, and preparing to conduct, military operations according to information -related principles. It means disrupting, if not destroying, information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threat to counter first, and so forth. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the balance of information and knowledge in one's favor, especially if the balance of forces is not. (Arquilla and Ronfeldt 1993, p. 30)"

Three key concepts may be deduced from Arquilla & Ronfeldt's description of cyberwar:

1. information is central to cyberwar activities,
2. the purpose of cyberwar is to effect the adversary's kinetic military capabilities, while protecting your own,
3. it is important to effect decision making to understand the impact of a successful cyber attack both offensively *and defensively*.

Cyber warfare has broad implications for both military organization and warfighting doctrine (Arquilla and Ronfeldt 1993, pp. 24-25). The technologies employed in cyber warfare can provide the commander with *topsight*. Topsight is a greater understanding of the big picture and improved situational awareness of the battlespace. It delivers improvements to the decision-making processes by providing a more clear picture of battle space capabilities through both a more accurate picture of the enemy and *friendly* force capabilities (Arquilla and Ronfeldt 1993, pp. 30-31).

In cyber warfare, however, gaining topsight may not be easy. According to Gruber, a lack of deliberate planning to employ cyber technologies to objectives has traditionally hindered the full realization of the capabilities offered by these technologies (Gruber 2000, pp. 8-12). The key to being successful in the continually evolving domain of cyberwarfare operations is to continually re-examine the existing paradigm and adjust as necessary. If areas of improvement are identified, the organization must strive to meet those needs. Such an area with a need for improvement is providing the military commander with the topsight needed to understand how a successful cyber incident has impacted his/her ability to carry out the mission.

The Evolution of Military Dependence on Cyberspace.

Cyber warfare is a serious matter in military circles as more military operations continue to depend on computer networks and cyber space (Kumagai 2003, pp. 118-119). The first step in understanding how the Air Force approaches cyber information security is to "gain a common view of how information has grown into a critical component that directly affects the conduct of military operations (Gruber 2000, p. *iii*)." From the

earliest military operations, information has been a key factor to success in warfare. Human history provides a nearly endless set of examples of the army with the superior information advantage winning the battle. In his forward comments, prefacing Air Force doctrine, General John P. Jumper states that those with a "superior ability to gather, understand, control, and use information" maintain this advantage on the battlefield (AFDD2-5 2005). America has traditionally been the leader in employing cyber-based information technologies to gain and exploit such an advantage in the battlespace. As the technology evolves, so must our understanding of how to best employ this technology to fully exploit the cyber-based information assets gained from our adversaries—and our own. It is important to understand how we arrived. Sometimes we can learn from the problems of the past to improve our future. Much is written about the evolution of information technology, the emergency of the Internet. This sub-section concisely describes the gradual infusion of military operations into cyberspace.

The DoD embarked on its first large-scale attempt at integration of computers, satellites, and communication systems with the issuance of DoD Directive S-5100.30, titled "Concept of Operations of the Worldwide Military Command and Control System (WWMCCS). WWMCCS, although never fully integrating all functions of command and control, was the first large scale system designed to link information-bearing technologies to provide increased situational awareness to military commanders (Gruber 2000, pp. 4-5). Allard notes that WWMCCS development was influenced by the rapid and novel availability of both technology and resources to meet the requirements of the individual unified and specified commands, rather than by specified strategic goals (Allard 1990, pp. 133-135). The importance of WWMCCS to this research is that it

foreshadows the vulnerability of kinetic operations that depend upon digital information, as several real world mission complications resulted from WWMCCS computer outages (Allard 1990). This may be the first time that the military realized degradation of operations capabilities directly attributable to the failure of computerized processing systems.

The next milestone on the journey to technology-dependence was the emergence of networks, which eventually lead to the creation of cyberspace. Integration of military operations and computer information systems had grown silently and steadily in the previous decades, but the promise of increased efficiency through new networking technologies and the Internet encourage the Air Force to embark in a characteristic rush to new incorporate these new technologies; reintroducing many of the problems experienced with the WWMCCS program. This dependence of the flow of digital information and information technology was soon apparent in the evolution of the military as an expeditionary force with new and sophisticated weapons systems that pushed the envelope of the existing cyber-infrastructure (Gruber 2000, p. 16).

The already straining infrastructure was quickly further burdened by the new emphasis in information warfare. Gruber observes that there was little forward planning for fitting technology to objective, and the result was a reduced ability of the DoD's infrastructure to support fully support combat operations. The underlying reason was that the DoD's approach to information warfare forced a focus on watching for hostile computer attacks, which inhibited efficient information flow from CONUS to forward operating locations. (Gruber 2000, pp. 19-21). To correct this problem, Gruber makes several suggestions, some of which we seen implemented in 2004 and continue to date;

as witnessed within the United States Air Force by the creation of the Air Force Network Operations and Security Center (AFNOSC) (AFI 33-138 2004), consolidation of Air Force networks under a unified network operations command and control structure.

The DoD has recognized many of the problems observed by Gruber and others and has made similar shifts in control and configuration of information infrastructure on which military operations are now so intimately dependent. The Global Information Grid is a product of this shift and a clear indicator that the DoD recognizes that the military's "ability to leverage the power of information will be key to our success in the 21st century (Grimes n.d.)." The GIG vision is to overcome the problems described by Gruber by providing user with a seamless, secure, and interconnected information environment for both the *warfighter* and the authorized business user (NSA n.d.).

This carries with it a heavy implication of the level of dependence the military, and indeed the nation, has on the information flow of cyberspace. In a study performed on the cyber warfare means and motivations of selected nation states by the Institute for Security Studies at Dartmouth College, Billo and Chang identify three general areas of vulnerabilities to national security of the United States exploitable through cyberspace operations. These are:

1. the United State's critical infrastructure,
2. its economic and financial sector,
3. and the military and national security sector (Billo and Chang 2004, pp. 130-131).

Billo and Chang cite the modern military's high level of reliance upon cyberspace assets is opening up "more holes in critical military infrastructure. (Billo and Chang 2004, p. 131)" Billo and Chang further state that:

> "Much of the Pentagon logistics chain flows over public-switched networks. Some of the intelligence gathering of U.S. intelligence agencies also flows over public networks. Secure IT is critical in making sure that the data received on both ends of an intelligence transmission is not compromised (Billo and Chang 2004, p. 131)."

There can little serious disagreement that the United States military relies more heavily upon cyberspace than ever before and will continue to do so into the near future. Drucker's (1993) assessment that every organization is an now an information organization rings especially true for the modern United States military. Many realize that our military operations are vulnerable and defensive cyber operations must evolve at a rate commensurate with our adversaries and ensure we are prepared to defend against a cyber attack (Winkler, O'Shea et Al. 1996, pp. 2-4).

The Kinetic Impact of Cyber Attacks.

> *"This is the first time in American history that we in the federal government, alone, cannot protect our infrastructure. We can't hire an army or a police force that's large enough to protect all of America's cell phones or pagers or computer networks."* Comments of Secretary of Commerce William M. Daley (2000) regarding cyber protection

It is commonly accepted that cyber attacks can affect real world functions and activities, but a debate exists over the *extent* to which the effects of cyber-induced damage may be realized in the real world. Billo and Chang observe that the community of cyber-security *experts* holds widely ranging opinions on this issue. Some experts feel

that an *electronic Pearl Harbor* is impossible while others herald that such a catastrophe is inevitable (Billo and Chang 2004, p. 12). James Lewis, a senior fellow and director of technology policy at the Center for Strategic and International studies, made the following statement regarding the impact of a cyber attack:

> "Nobody argues -- or at least no sane person argues -- that a cyber attack could lead to mass casualties. It's not in any way comparable to weapons of mass destruction. In fact, what a lot of people call them is "weapons of mass annoyance." If your power goes out for a couple hours, if somebody draws a mustache on Attorney General Ashcroft's face on his Web site, it's annoying. It's irritating. But it's not a weapon of mass destruction(Lewis 2003)."

In this interview Lewis also makes the following argument against the vulnerability of national infrastructure to a cyber attack:

> “The other thing you can look at is, we know what attacks on critical infrastructures are like. This is something the military has been doing for at least 80 years. What we've discovered is it's hard to knock out an infrastructure. Nations are a lot tougher than they look. You can put something out for a couple of days, and people work really hard to get it back online. So this isn't an easy task when you're using high explosives, and high explosives do permanent damage, unlike cyber attacks, which are not anywhere near as threatening (Lewis 2003).”

Lewis is not alone in his view that the impact of a cyber attack is grossly inflated. Joshua Green, an editor for Washington monthly states:

> “There is no such thing as cyberterrorism--no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity. What's more, outside of a Tom Clancy novel, computer security specialists believe it is virtually impossible to use the Internet to inflict death on a large scale, and many scoff at the notion that terrorists would bother trying (Green 2002).“

The literature review accomplished in this research begs the question, *where are Green's* many *scoffers?* The vast majority of literature available on this subject does not support the view of Lewis and Green. It should be noted that their point of view glosses over a universally agreed upon issue that America is the world leader in dependence on cyber-based information, with as much as 95% of networks being connected to each other in some way (Billo and Chang 2004, pp. 14-17).

And the degree of the dependency increases annually. In interview with GCN magazine, Sami Saydjari, CEO of Cyber Defense Agency commented on this recent explosive growth.

> "Twenty years ago, the infrastructure operated separately from the Internet and other open networks. So in some sense, the level of vulnerability has gone up simply because the level of interconnectedness has gone up significantly (Jackson 2006, p. 20)."

Billo and Chang point out that the experts with access to classified information sources express concern that "the growing tendency in advanced industrial economies to link internal business management tools and administrative controls to the Internet could be catastrophic for overall U.S security (Billo and Chang 2004, p. 12)."

Indeed, even skeptics such as Washington Post writer Chris Suellentrop, who called the idea of cyberterrorism both a hoax and a conspiracy by the technology companies to generate large profits, become convinced of the reality of the national vulnerability when seeing the extent of American critical infrastructure dependence on cyberspace up close. After participating in a cyber terrorism exercise conducted by Dartmouth Institute for Security Technology

Studies, he realized the gravity of the vulnerabilities presented by cyberwarfare, reversing his opinion and going from “smarty-pants to scaredy-cat (Suellentrop 2006).”

Recent research studied the costs to the U.S. economy from damage caused by a successful large scale, well targeted cyber attack and produced disturbing findings. Dynes’ study, *Costs to the U.S. Economy of Information Infrastructure Failures* (Dynes, Andrijcic et Al. 2006) examined the *ripple effect* a catastrophic cyber attack and determined that would cost the economy millions of dollars for cyberspace disruptions greater than a few days. The study noted that a growing reliance on networks would result create the possibility for even greater impact in the future (Dynes, Andrijcic et Al. 2006, p. 20). In February 2002, a group of 54 distinguished Information Assurance professionals drafted and signed a letter for President George W. Bush expressing a deep concern over the large and continually growing risk to the nation from a danger potentially more devastating to national morale and the country’s economy than the 11 September 2001 terrorist attacks (PCD 2002a).” Richard Clarke, who served as the White House Cyber Security Advisor from October 2001 to March 2003, expressed great concern about the vulnerability of the United States to cyberwarfare, and made the following statement in an interview with *PBS Frontline*:

> “We, as a country, have put all of our eggs in one basket. The reason that we're successfully dominating the world economically and militarily is because of systems that we have designed, and rely upon, which are cyber-based. It's our Achilles heel. It's an overused phrase, but it's absolutely

> true….some enemy some day was able to come around and knock the whole empire over." That's the fear (Clarke, 2003)."

Michael Vatis, the Director of the Institute for Security Technology Studies at Dartmouth College, and director of the Institute for Information Infrastructure Protection (I3P) supports this view and states:

> "America remains highly vulnerable to another form of attack: a "cyber attack" against the computer networks that are critical to our national and economic security. Attackers might target banking and financial institutions, voice communication systems, electrical infrastructures, water resources, or oil and gas infrastructures. The growing complexity and interconnectedness of these systems renders them increasingly vulnerable to attack. While a physical attack is likely to be carried out only by terrorists or hostile foreign nation-states, cyber attacks may be carried out by a wide array of adversaries, from teenage hackers and protest groups to organized crime syndicates, terrorists, and foreign nation states. As a result, the problem is of enormous breadth and complexity (Vatis 2002, p.3)."

Certainly, the majority of literature publicly available serves as worthy and suitable evidence of the American vulnerability to a large and well-targeted cyber attack. Considering that the experts closest to the problem, with presumably the better view of the dependencies and vulnerabilities within the American critical infrastructure and military operations, there can be little serious argument whether cyber-based attacks can cause impact kinetic activities in the real world.

The extent of impact varies on the type of cyber asset successfully attacked and the degree of dependency the real-world function has on it. It follows, therefore, that the better civilian and military decision makers know the potential impact when key cyber-supported systems are lost, the better prepared

America will be to recover. This fact underscores the need for development of an effective cyber-damage assessment framework.

Threats to Cyber Assets.

Organizations that rely on cyber information face daily threats that could damage or destroy these information assets on which mission operations rely. In an environment where loss of critical information can result in loss of operational capability, it is important to understand threat. Threats originate from both inside and outside the organization, and can be man-made or may be caused by an unpreventable disaster (Petrocelli 2005, p. 5). This section will discuss some of the common forms of threats to an organization's information assets.

Outsider Threat.

The term cyber attack generally brings to mind malicious activity from outside of the organization. Too often generalized as "*hackers*" by the uninitiated, outside threat actors come in many flavors ranging from nation states, organized crime, *cyberterrorist*s, and "*hacktivists*". They share a common goal of either directly attacking cyber information assets, or its *container*, the system on which the information asset resides (Stevens 2005, p. 5). The motivation, for each varies widely. Organized crime and *cyber cartels*, generally motivated by financial gain, often target cyber information assets of banks or other e-commerce sites to engage in a variety of illicit activities ranging from theft to extortion by holding to hold the victim information or systems for "ransom" (Winkler 2005, pp. 71-74). "Hacktivists" and *cyberterrorists* generally attack cyber assets to promote political, ideological, theological, or similar causes. Denning observes that the boundaries between the two latter groups are fuzzy (Denning 2001, p. 241).

Nation states may attempt to cripple American military and civilian command and control structure via external cyber operations (Shimeall, Williams et Al. 2002).

Despite the best efforts to keep the outside actors on the outside, there are countless examples of successful intrusion, with many causing damage measured in millions of dollars (Tiboni 2005a). In 2001, a Connecticut teenager hacked a presumed secure Air Force system that tracked the positions of Air Force planes worldwide causing more than $66,000 damage (Rosencrance 2001). The year 2005 was both the widely publicized hacking of the Air Force Personnel Center (AFPC) data base in which 33,000 Air Force officers was compromised (Mark 2005), and the less publicized but no less dangerous onslaught of "attacks: against United States critical infrastructure and military networks (Graham and Eggen 2005). Both examples serve to illustrate the targeting of cyberspace information assets either directly or indirectly targeting information by attacking the infrastructure that contains the asset. These indirect attacks against the asset's container, attempt to affect the organization's ability to use the asset effectively. Each type of attack bears the potential of causing some degree of mission degradation, whether damage and mission impact realized or not.

Inside Threat.

Chinchani, et. Al, define the insider as a legitimate user who leverages system privileges, "familiarity and proximity to their computational environment to compromise valuable information or inflict damage (Chinchani, Iyer et Al. 2005, pp. 108-109)." Existing literature agrees to the spirit of this definition. Insiders have rapidly come to be considered "one of the most challenging problems facing the security of information systems today (Butts 2006, p. ii)" For the past several years, the CSI/FBI survey has

reported a decline in the number of reported insider incidents (Gordon, Loeb et Al. 2006, p. 13). This, however, is not a reliable indication of the threat, as damage caused by inside threat actors can be severe; accounting for more than 80 percent of annual losses in some organizations as shown in Figure 2 below. In a military environment where the economic impact of a cyber security incident is secondary to the impact upon operational mission capability the effects of insider activity may be catastrophic; as demonstrated when insider activity resulted in more than 36 hours of mission stoppage on Coast Guard networks (DiDio 1998). Research on detecting and preventing insider activity continues to emerge, such as the Butts' methodology (Butts 2006) for formalizing the inside threat to identify high-probability inside threat actors. Regardless of preventative measures, inside threat actors will inevitably occur making the need for a defensive cyber damage assessment framework even more important.

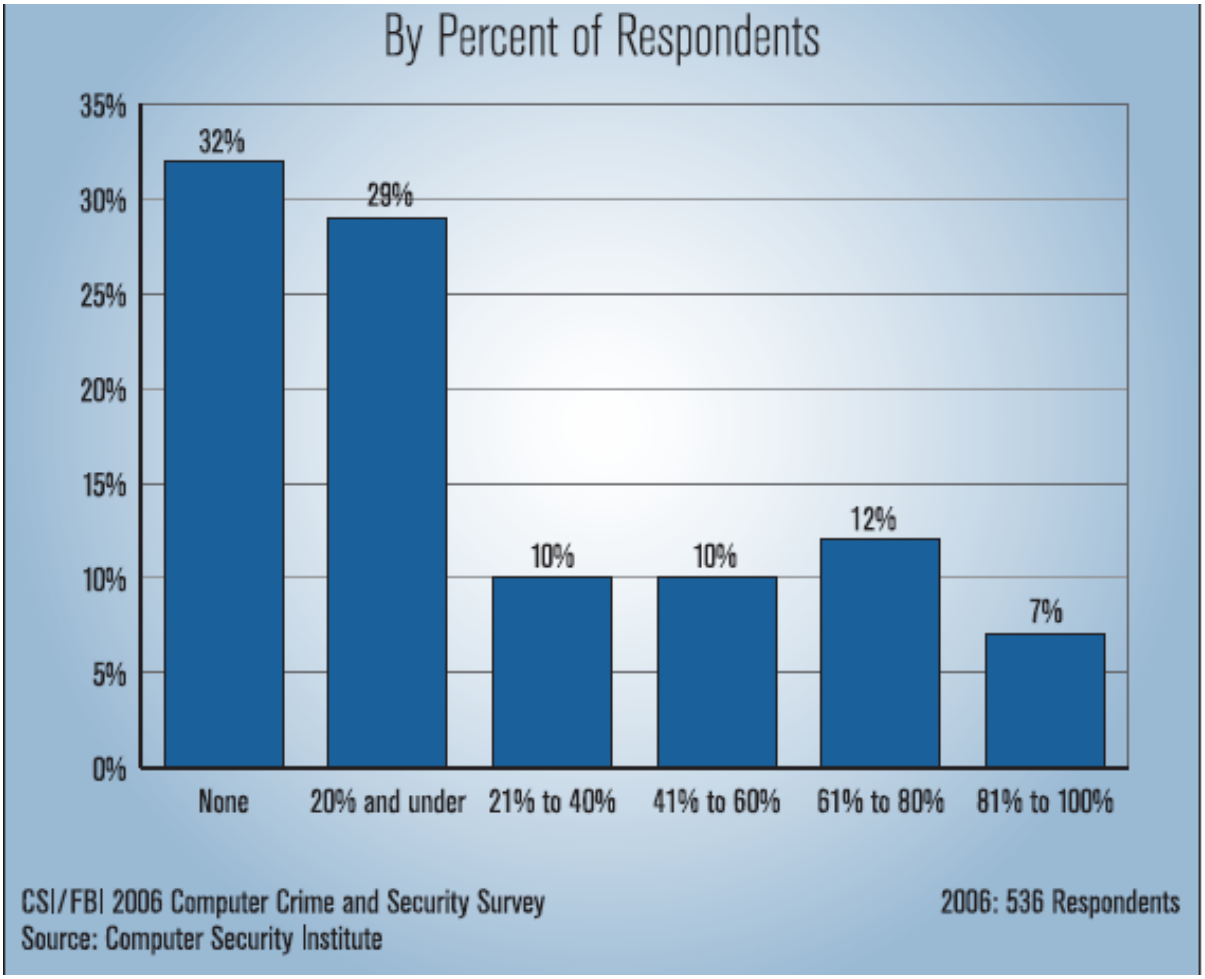


Figure 2. Percentage of Reported Loss from Insider Threats (Gordon, et. Al 2006, p. 12)

Human Accident and Natural Disaster.

Not all threats to cyber assets are necessarily malicious in nature. Baskerville observes that many times cyber security programs focus too exclusively on malicious activity. Important threats, such as the potential for human error and harm caused by accident, are excluded from the organization's risk assessment. Such exclusion allows the effects of accidents introduce overlooked threats and vulnerabilities to the organization's critical cyber information assets (Baskerville and Im 2005). *Mistakes* and

slips by system or software developer and/or users can unintentionally create a mission impacting catastrophe or introduce security holes which allow unauthorized and potentially damaging activities to be carried out by malicious threat actors (Norman 1983, pp. 254-255). Human accident, while not malicious in nature can have the same impact on mission capability as a malicious attack.

Natural disaster is another area that Baskerville charges as overlooked by many security programs. As with human error, natural disaster can introduce exploitable vulnerabilities, or more often act as an independent agent to impact the ability of cyber security to function as expected (Baskerville and Im 2005). Recent natural disasters, particularly Hurricane Katrina documented the vulnerabilities of our cyber-based information systems and demonstrated both how quickly an information infrastructure could be taken out and how a program that does not plan for these non-malicious events can find itself unprepared when natural disaster occurs (IEEE-USA 2006).

An Incident Taxonomy.

An organization with a limited scope of risk to its assets can find itself unprepared when a risk is realized from a vector beyond the organization's scope of assessed risk. This is especially true of organizations that plan for risks based on threat scenarios (Soo Hoo 2000, p.11). Unfortunately, many widely accepted threat and incident taxonomies maintain a relatively narrow scope on risk. One such widely cited taxonomy model is the Computer and Network Incident Taxonomy (see Figure 3 below) proposed by Howard and Longstaff (1998, pp. 15-17).

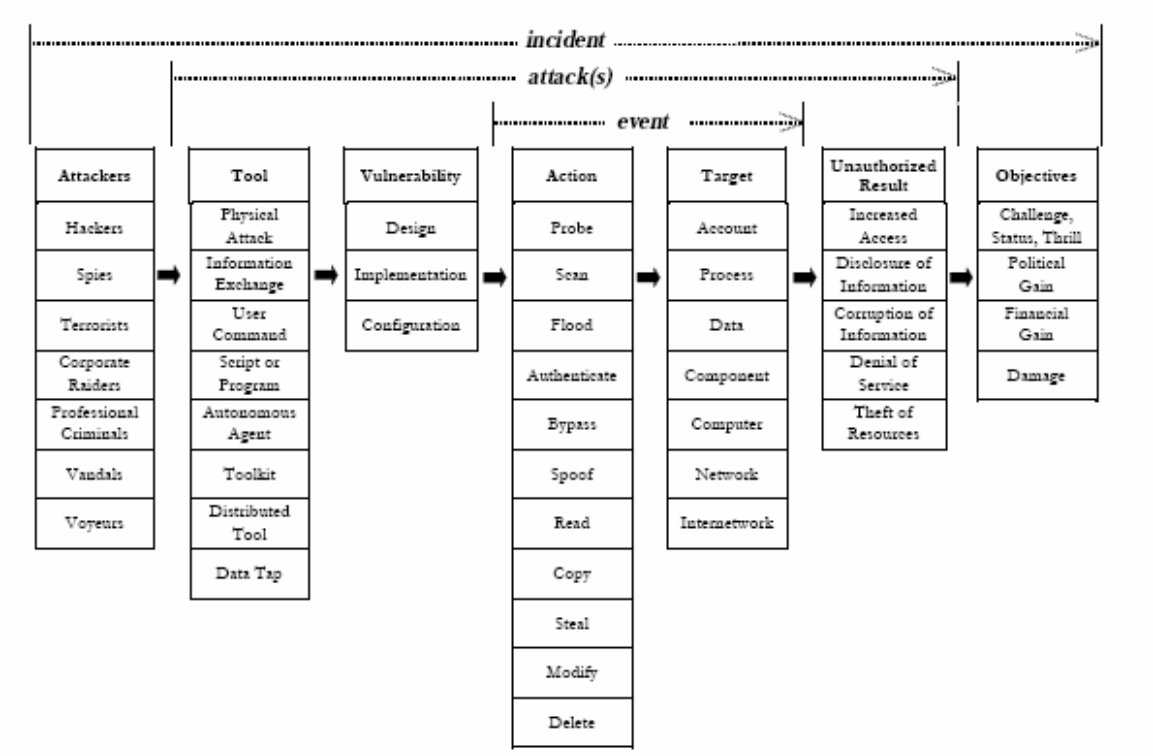


Figure 3. Howard's Computer and Network Incident Taxonomy (1998, p. 16)

Section Summary.

Cyberspace is more than just the Internet. It is all the space between networked computers where digital information is exchanged. Cyberwarfare is a critical part of information warfare and IO that occurs in cyberspace. Cyberwarfare activities can have kinetic effects on organizations whose operations rely on the information assets of cyberspace. Military operations have developed a strong and ever-increasing dependence on cyberspace; which has introduced new vulnerabilities to new threats both inside and outside the network. These threats can come from a variety of vectors, and a good security program must plan for all forms of threats to protect the cyber-based assets on which modern military operations depend.

It is important to rely on a threat or incident taxonomy model the captures as wide a spectrum of risk as possible. It is also important that the taxonomy recognize the value of information as an asset. All cyber attacks against an organization are attacks on its information assets to some degree. These attacks produce second and third order impact effects that the organization must address.

Foundations of Defensive Cyber Damage Assessment

Military theorist and United States Air Force Colonel John A. Warren wrote that the commander is the center of gravity for all military campaigns. Command, itself can be broken down into three basic functions: information, decision, and communication. He states that one of the keys to effective command is exploiting an awareness of *both* sides of the front (Warden 1988). Defensive cyber damage assessment is intended to be an exclusive form of *mission capability* assessment to provide the commander with awareness of how a successful cyber attack on his own networks has impacted his mission operations capability. Research in this area is sparse. What research is available is designed for assessing financial losses resulting from an attack; a measurement not useful for decision makers in organizations not driven by other than profit. Cyberspace operations affect both the cyber domain and the physical domain. The reliance of military operations upon cyberspace establishes the need for a defensive assessment framework to provide commanders with the battlespace awareness needed to prosecute the modern campaign. Surprisingly little research has been carried out towards establishment. This section will examine literature supporting the necessary foundational concepts need for CDA-D/MIA framework development.

Battle Damage Assessment.

Assessing the affects of actions against the adversary has been a critical factor in the outcome of battles and wars since the beginning of military history. Battle damage assessment (BDA) continues to play a pivotal role in command decision making in modern military operations. JP 1-02 provides the following definition for BDA:

> "The timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators (JP 1-02 2006)."

Early battle damage assessment was simple but became more complex as the complexity of war grew (Diehl and Sloan 2005, pp. 59-60). The technology of warfare allowed faster conduction of military operations, which called for the commander to make more decisions in ever shortening time constraints. Unfortunately, the limitations of the existing BDA paradigm began to show. The DoD's *Final Report to Congress: The Persian Gulf War, 1992* stated that traditional BDA methodology as it was employed in the Persian Gulf War was "too slow and inadequate". Changes were needed to improve the efficiency of the BDA structure (DOD 1992)." Lt Col Hugh Curry (2004)echoed this sentiment argued for the use of cyber technology to improve the timeliness of the BDA process.

In 2004, Lt. Col Michael Masterson discussed an improved conceptual BDA framework to provide commanders with improved battlespace awareness

through assessing the *effects* of actions against the enemy. Combat assessment (CA) is defined by JP 1-02 as "[t]he determination of the overall effectiveness of force employment during military operations (JP 1-02 2006, p. 97)." Put another way, CA is the overall assessment of combat operations in relation to the intent of the command objectives, of which BDA is only a part (Sopko 1999). Masterson states that CA is a hierarchy of assessment that begins with Tactical Assessment (TA) where BDA occurs. TA supports component commander's Operational Assessment (OA), which in turn supports campaign assessment, which is the joint force commander's assessment the state of overall campaign mission (Masterson 2004).

Masterson's description of the hierarchy of assessment bears an analogous relationship to the hierarchy of missions discussed in the previous chapter (Alberts and Dorofee 2005, pp. 3-4); and is a important concept to defensive cyber damage assessment. Sopko, while citing problems with CA that affect the Joint Air Operations Center (JAOC) makes the following important differentiation between CA and BDA that will have strong ramifications for the development of CDA-D/MIA methodology:

> "The most common mistake among operators and intelligence support personnel alike is the confusion between BDA and CA. BDA is a familiar term with historical roots and tends to overshadow the CA process. Unfortunately, BDA is just one part of this process. BDA is intelligence driven while CA is the responsibility of the commander. BDA focuses damage to the target and target system while CA is much broader and tries to answer the question: "how well are we doing and what's next?" Like BDA, CA provides information to commanders, battle staffs, planners, and other decision-makers. This wide audience complicates definitions and functions as it is applied across all components and joint staffs. The bottom line is that this audience must understand what type of information they need. Commanders must be educated in the process and be able to practice this. All too often, CA is an afterthought. CA must be

considered in the beginning of the targeting process with the development of the commander's objectives. (Sopko 1999)"

Defensive Damage Assessment.

BDA as previously defined by JP 1-02, attempts to build "timely and accurate estimate (2001, p. 63)" of effects of offensive actions against an adversary. Conversely, *defensive damage assessment* seeks to provide the same type of estimate of the effects of an enemy's attack on friendly assets. The goal of defensive cyber damage assessment is to assess the degree of degradation to one's own mission capability resulting from a successful cyber attack. In the private sector, such loss of mission capability may be measured in financial loss and related constructs, such as those discussed in the Horony model (Horony 1999) which discussed later in this paper. In military operations, however, factors such as customer loss, business expenses, and damage to reputation do not provide the commander with the situational awareness required to make smart and timely decisions in wartime.

In military operations, commanders must make binding decisions that affect the overall success of a battle or campaign. Defensive cyber damage assessment must provide the commander with timely and accurate assessment of any degradation in operational capability resulting from a successful cyber attack, which may impede his force's ability to carry out the operational intent. Failure to perform self-assessment accurately following a successful cyber attack may introduce unnecessary risk and error into the commanders' decision-making process.

The lack of a self-damage assessment model was an issue discussed more than a decade ago, when Alberts recognized the serious deficiency in the DoD's ability to assess

the damage resulting from a successful compromise of friendly cyber assets (Alberts 1996, p. 24). Today, literature on defensive cyber damage assessment remains relatively scarce considering the awareness of the exploitable vulnerabilities of business and national infrastructure. Available research literature nearly exclusively addresses private sector economic interests; with cost loss determination being the focal point of damage assessment. Even research attempting to determine impact in an academic environment (Rezmierski, Deering et Al. 1999) elects economics as the impact metric of choice. Although establishing an effective CDA-D/MIA framework that is suitable for damage and mission impact assessment of military operations encounters many problems and challenges cited by Sopko (Sopko 1999), the issue is important enough that it must be accomplished. When doing so, it is important that the approach to damage assessment is correct to ensure delivery of the right damage and mission impact assessment metrics to the military commander.

Decision Superiority.

Air Force doctrine describes decision superiority as being able to employ the constructs of decision making faster and more effectively than the adversary. Decision superiority provides an advantage in the real world and cyber battlespace by allowing commanders to exploit a superior situational awareness of the battle space. This situational awareness enables commanders and their forces to make and implement better-informed and smarter decisions faster than can the adversary (AFDD2-5 2005). The Air Force utilizes the well-known "OODA loop" as a grounded decision-making model. The OODA loop is a theory developed by retired Air Force Col. John Boyd that asserts that all rational human behavior can be modeled as a continual cycling through four distinct tasks: Observation,

Orientation, Decision, and Action (OODA). According to Boyd (1996) , the key to competitive success is operating inside opponents' OODA loops. The Air Force has developed an adaptation of Boyd's OODA loop to match its revised doctrinal concept of decision making in the IO environment (see Figure 4 below). This model provides both a picture of the IO environment and a logical foundation for the constructs of IO capabilities in the information environment as it relates to Air Force IO doctrine.

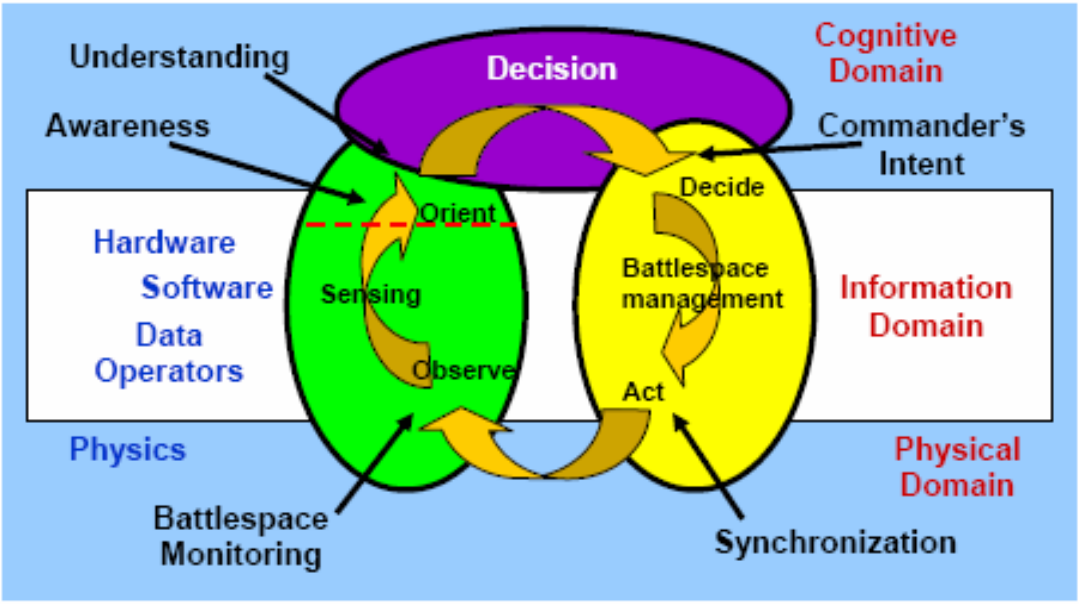


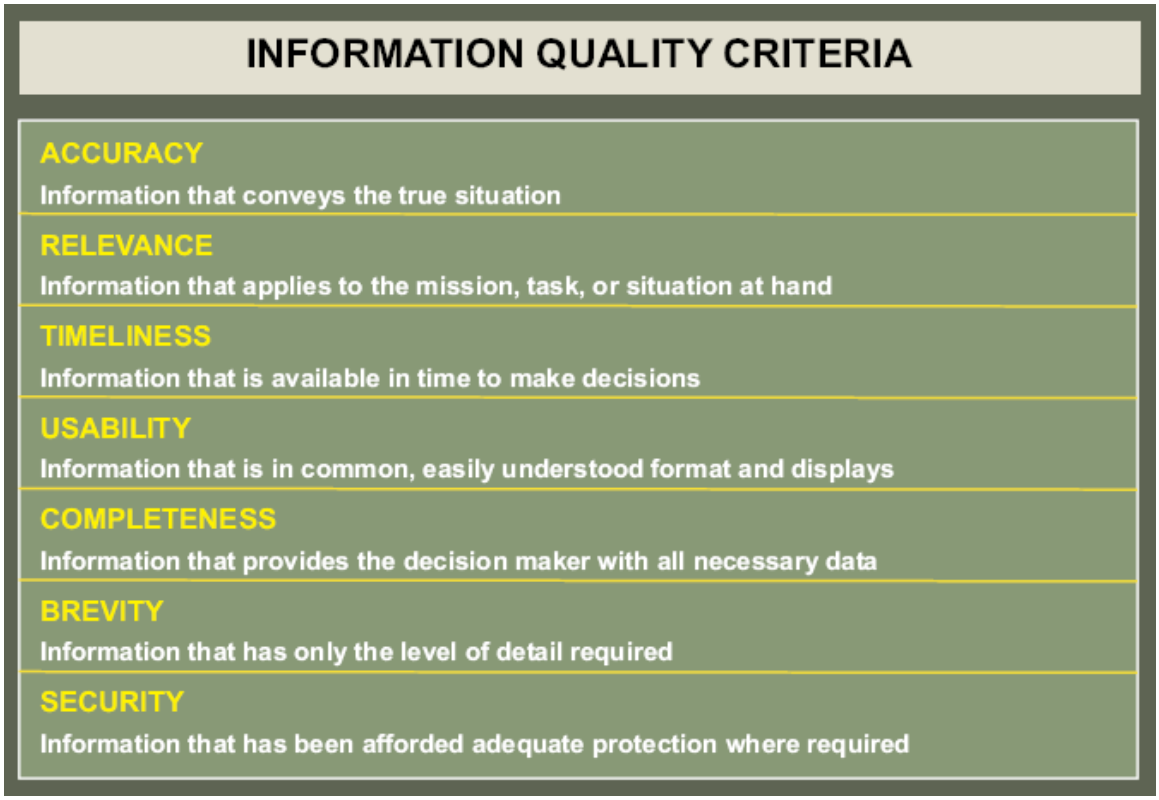
Figure 4. Decision Making in the Information Environment (AFDD 2-5 2005, p. 3)

Information Quality.

Joint Publication 3-13 explicitly states that "information is a strategic resource vital to national security (JP 3-13 1996, p. *ix*) " The information that is used for making important mission decisions depends that the information is of high quality suitable for such use. The criteria for quality information chart provided by JP 3-13 builds a solid foundation for determining the type of information to be presented in a damage and

mission impact assessment report (see Table 1 below). The information in this report must be all of these things to allow the commander to make smart and timely decisions about issues that may arise following a successful cyber incident.

Table 1. Information Quality Criteria



(JP 3-13 1996, I-3)

Development of Damage Metrics.

Military operations supported by cyber technology can provide commanders a distinct advantage by equipping them with timely information. Too often, though, military decision makers find themselves presented with the wrong information on which to base timely and smart decisions. When performing effective defensive cyber damage assessment after successful cyber attack, it is supremely importance that the

organization's decision maker is presented with a timely and accurate assessment of any impact to mission capability. In other words, to be effective a defensive damage assessment model must measure the right thing in the right way so that the result can be used effectively by the commander. Doing this begins with creating the appropriate metrics.

Although metrics are generally applied to process improvement, this research borrows some of the important concepts in metrics development. According to Wesner, metrics must first and foremost measure the right thing (Wesner, Hiatt et Al. 1995). In other words, the measurement must be bound to a goal or objective. In BDA this may be a measure or performance (MOP) – measuring the efficiency of a task's ability to meet an objective; or it may be a measure of effectiveness (MOE) – how efficient a task was in doing the right thing (Masterson 2004). MOPs and MOEs intend to measure the "right" things to provide battlespace awareness; defensive cyber damages assessment must do the same thing. Metrics must also be *SMART: specific, measurable, actionable, relevant, and timely* (Wesner, Hiatt et Al. 1995). Each these constructs must be considered to develop an effective defensive cyber damage assessment framework which provides decision makers with the right information following a cyber compromise. An effective defensive damage assessment framework can be crucial to giving the organization's decision makers decision superiority. Indeed, determining what the organization's decision maker *needs* to see for decision superiority in the battlespace must be a primary driver for developing assessment metrics.

Information Saturation.

IT and cyberspace can provide the organizational decision maker, and particularly the military commander, with the capability to have all the right information at arm's length almost instantaneously. In this way, IT affords the decision maker a tremendous advantage when desiring to attain decision superiority. However, effective and *smart* decisions depend on having the right quantities of the right input information, meaning accurate and relevant information, to facilitate option development needed for effective decision making. In accurate or incomplete decisional input, the wrong amount of input, or a combination of both produces what is colloquially known as *garbage in garbage out* decision making (Bowman and Moskowitz 2001, p. 775).

Providing the decision maker with input information of insubstantial quality or quantity will increase the probability of a bad decision. Often overlooked, however, is the fact that too much information can have a similar effect on decision making; even if the information is correct and suitable to the situation. Jensen observes that "too much information leads to incapacitation of the decision maker's ability to make a timely decision. Information age leaders must caution themselves about this possibility. Sensory overload represents our human limitation to process information. Increased volume overwhelms not only our ability to consume, but also our ability to process and understand (Jensen 2005, p. 56)."

In a time when many military leaders are calling for more real-time information about the battle space, it is important that the right amount about the right things are provided to them. To much complex information can produce the same effect as no information. Therefore, an effective defensive damage assessment framework must

assess the damage following a cyber security incident, estimate the impact to mission capability, and report it in a manner that provides the decision maker with the right quantity of information on which to make a required decision. Above all the information prevented to the decision maker must be presented in a way the delivers the mission impact message in a simple and easy to understand format. Otherwise, such reporting could become white noise in the sea of information provided to the commander.

Critical Information.

According to Joint Publication 3-13.3 (1996), Operations Security (OPSEC) is a process that identifies critical information to determine if friendly actions can be observed by the adversary to exploit vulnerability in friendly operations (p. *vii*). This program requires that organization critical information lists created for the commander to understand which information resources he/she must protect (p. I-6). The OPSEC program is not a suitable for vehicle for documenting cyber information assets.

The intent of the OPSEC program is not to document potential cyber risk. The program possesses a *Global War on Terror* (GWOT) risk focus. In the early part of the GWOT, there was great concern about the large pools of personal and organizational information freely accessible through the Internet. Information such as personal information, street addresses, maps of facilities, and locations of critical buildings of military and critical infrastructure organizations were freely available to anyone with Web access.

OPSEC efforts almost entirely omit cyber information assets and there is no valuation process within the program. As a result, the current OPSEC program implementation is not designed to provide a commander effective mapping from

information assets to operational or mission impact; a problem that caused by the type of information collected. Critical documentation of cyber information is simply not available for damage and mission impact assessment efforts.

Damage Assessment Reporting.

The purpose of a CDA-D/MIA framework is to provide the organizational decision makers with the appropriate situation awareness of impact to mission capability to enable and maintain decision superiority in the battle space. Literature review thus far has established that this is one way in which CDA-D/MIA bears a close relationship to BDA. However, without an effective mechanism to get the assessment report to the decision maker, there is little advantage in performing assessment, as was learned in the problems with BDA during the military operations of recent years (Curry 2004, p.13-15; Diehl and Sloan 2005, p. 60). The Air Force, and each respective service, has fortunately established such a mechanism. Air Force Instruction (AFI) 33-138 sets cyber incident reporting procedures within the Air Force networks and facilitates linking to GIG command and control functions. AFI 33-138 is discussed in detail later in this paper.

Unfortunately, personal experience in the Iraq Theater of Operations in 2004 demonstrated that the existing incident reporting structure at the time was not sufficient to get the right information to the decision makers in a timely fashion. The development of a standardized and validated CDA-D/MIA framework that can be integrated into joint and service defensive IO components on DoD networks may help to correct these deficiency in future military operations.

Damage Assessment versus Mission Impact Assessment.

Damage assessment is only part of the picture. Damage assessment in the cyber realm is an inherently focused on technological assessment concerned primarily with rapid system restoration issues (Lala and Panda 2000, p. 300). The Air Force Computer Emergency Response Team (AFCERT) stood up in 1993 with the mandate of incident handling responsibilities on Air Force networks, including incident damage assessment (FAS 1997). Recent research (Thiem 2005) underscores the many problems with damage assessment efforts on Air Force networks, such as lack of standardization and validation damage assessment throughout the Air Force enterprise.

Damage assessment however, is only a step towards the more recent and more operationally important problem with mission impact assessment. According to Arvidsson, cyber damage is a consequence of "an attack that affects the normal operation of a system or service. (Arvidsson n.d.)" Impact is the result of damage caused by the attack "in terms of the user community (Arvidsson n.d.)." These definitions reflect the common perception of damage and mission impact assessment, which leads to confusion between the two.

Damage assessment and mission impact assessment must not be viewed as the same thing. Damage was previously defined as a reduction in value resulting from some external action (Oxford, 1986). Damage assessment, then, must be concerned with determining damage in *terms of value loss* resulting from an incident.. This loss must be assessed in terms relevant to the organization. Mission impact must be viewed as an evaluation of how the *damage*, or loss in asset value, impairs or potentially may impair the organization's mission operations.

Damage assessment and mission assessment are not the same process, but they maintain a dependent relationship in that damage assessment must be accomplished to accurately understand mission impact resulting from a cyber incident.

Section Summary.

This section examined the foundations of defensive cyber damage and mission impact assessment by looking at literature on the key contributory issues to damage assessment. Battle damage assessment seeks to determine the effects of offensive actions against an adversary, and has much in common with defensive damage assessment. The purpose of both is to provide the commander with the battlespace awareness needed to make smart and timely decisions and achieve decision superiority in the battlespace. Both BDA and CDA-D/MIA face similar challenges to meeting this objective. Both processes are extremely important to achieving a battlespace advantage. However, unless the assessment process measures the right things and delivers the results to the commander in a timely and appropriate format, and in the right quantities little benefits may be seen to either process. Even with all these things done, the information must be presented to the decision maker in a way that it can be used and understood. The information in mission impact assessment reporting must be quality information to be suitable for making the right decisions in a timely manner.

Risk Management on Information Networks

The term risk management is widely used and has different meanings to different communities of interest (Kloman 1990, pp. 201-202). Risk management *is* the process of identifying and assessing the risks to the organizations information assets; and applying

appropriate mechanisms to reduce, manage and control risks to information assets (Bragg 2002). Many enterprises 'flirt' with the idea of risk management, but research show that few actually implement it correctly (Hampton 2006, p. 33). Research also demonstrates that organizations which fail to address risk will inevitably realize a greater degree loss than organizations which do (Whitman and Mattord 2004, p. 287). Risk management is the most critical component of security planning; consisting of three important activities in two distinct phases. The first two activities, risk identification and risk assessment, occur in the first phase. Defensive damage assessment exclusively concerned with the activities of this first phase. The third activity, risk control, solely comprises the second phase (Whitman and Mattord 2004, p. 321), and is beyond the scope of this research.

This section will discuss the main components of risk management and examine available literature on key approaches to risk management.

Threat, Vulnerability, and Risk.

The terms threat, vulnerability and risk are often confused and misused. Threat is the *potential* for violation of security that exists when there is a circumstance, capability, action, or event that could breach security and cause harm (SANS 2006). Vulnerability is a weakness in system security procedures, system design, implementation, internal controls, etc., that could *potentially* be exploited to violate system security policy (NCSC 1988). Risk is "an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result (Shirey 2000)." Risk can be viewed as a measure of potential loss to an organization; or more specifically, as a measure of *exposure* to damage or loss (see Figure 5 below). Two additional factors be satisfied: 1) there must be some uncertainty about the outcome, and

2) there must be some choice made about the course of action regarding the potential for loss (Alberts and Dorofee 2005, p. 5). Without the potential for loss, there is no risk (Petrocelli 2005, pp. 5-6). The magnitude of risk depends greatly on the assets at risk, or more specifically, the value of the assets at risk.

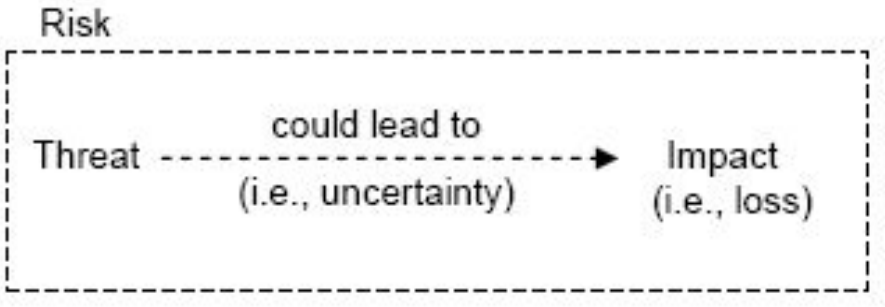


Figure 5. Threat and Risk (Alberts and Dorofee, p. 5)

The eighteenth century German scientist, Georg Lichtenberg (1775) once stated that, "Once we know our weaknesses, they cease to harm us." Risk actualization cannot be entirely avoided, but Lichtenberg was still partially correct. An organization that understands the relationship of threat, vulnerability and risk to its critical assets can do much to mitigate the damage and impact to the organization when risk becomes reality.

Risk Identification.

Risk identification is the process of self-examination in which the organization defines, identifies, and documents its information assets into useful groups (Whitman and Mattord 2004, p. 290). This process is not limited to simply risk and asset identification. The assets identified also are prioritized and assigned value in this stage. Risk identification can easily become a highly intensive task at the onset. Only by accomplishing this process, however, can an organization identify the assets vulnerable to

loss. This process lays the foundation for all future steps of risk management; and failure to effectively accomplish results in a greater probability of inefficient protection measures and an incapability to provide management necessary visibility into the impact following a disaster (Charron 1987, pp. 80-81). The risk identification process identifies critical assets. Critical assets are those assets that if damaged or lost would affect the organization's ability to operation efficiently.

Once critical assets are identified, they may be prioritized and valuated according to the respective 'worth' to the organization. This is done through categorization, classification, and determining the contextual value of each asset (Whitman and Mattord 2004, pp. 294-299). Classification can provide a baseline estimate, but the contextual value of the information asset is the most complex, yet most important of the asset constructs to determine (Petrocelli 2005, pp.181-182). Without accomplishing effective risk identification activities to identify and valuate critical information assets to be protected, no "target" exists for which to accurately identify and enumerate the vulnerabilities and associate threats to assets requiring protection. This is vital to any security planning effort.

Risk assessment.

It is possible for a system to appear safe, but actually have undetected vulnerabilities that put its assets at risk (Bishop 2003). There is little reasonable argument against risk identification and assessment as integral to establishment of the level of protection required to adequately protect organizational assets (GAO 2000). Whitman and Mattord (2004 pp. 290, 308) draw a distinct and important difference, however, between risk identification and risk assessment. Risk assessment can is the process of

analyzing threats and vulnerabilities of an information system and the potential impact of the loss of information or capabilities of a system. Risk assessment determines probable impact of loss of any asset identified in the risk identification stage (Whitman and Mattord 2004, pp. 308-309).

Approaches to Risk Management.

The past two decades have seen several approaches to risk management on information networks come and go. The first generation approaches, such as the Annual Loss Expectancy (ALE)-based "common framework" developed by NIST, failed. Kevin Soo Hoo (2000) attributes this failure to three fatal flaws: 1) an infeasible sized assessment task, 2) an expectation of deterministic values that resulted in an inability to handle uncertainty, and 3) required a large information harvest from a small field of data to populate the ALE model (Soo Hoo 2000, pp. 4-8).

Integrated Business Risk Management.

The second generation of approaches to risk management attempted to overcome the failures their predecessors. The *Integrated Business Risk Management* (IBRM) approach holds that IT risks are analogous to business risks, and can be managed in the same way. This approach is distinctly non-technical and focuses on the role of IT support for business goals (Soo Hoo 2000, pp. 9-10). Additionally, the IBRM implementation can be highly complex. While this approach is used widely in the business world, it may not be a practical for risk management of military networks. More importantly to this goal of this research, a central part of the IBRM approach focuses on return on IT investment, with securing information assets as a secondary consideration.

Scenario-analysis approach.

The *scenario-analysis* approach is possibly the most common risk management methodology. This approach focus on vulnerabilities within the security controls meant to protect the IT infrastructure. Although, in wide use within the DoD, scenario-analysis methodology suffers the major drawback of limited scope (Soo Hoo 2000, p. 11), focusing primarily on threat detection and exploit prevention through direct focus on technology. This focus on technical vulnerabilities makes establishing effective cyber damage assessment extremely difficult.

Value-driven approach.

Value-driven risk management approach is less complex than the IBRM approach and offers valuation-driven security specifications to information assets identified and valuated by an enterprise agent with sufficient perspective to determine relative value of the asset. These specifications attempt to ensure security and standardize security practices within the enterprise. According to Soo Hoo (2005), this approach avoids the technical complexities that crippled ALE-based methodologies, and facilitates focus on critical deployment issues. Soo Hoo argues, however, that this approach is too simple to be effective, ignoring key capabilities such as cost-benefit analysis and the information technology that contains the asset (Soo Hoo 2000, p. 10).

The OCTAVE method.

There are asset-focused methodologies, such as Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method (Alberts, Dorofee et Al. 2003), that overcome many of the shortcomings of other approaches by integrating attributes from other methodologies. The OCTAVE method was developed by Carnegie Mellon

University and allows organizations to balance the best practices of the previous three in one package (Whitman and Mattord 2004, pp. 347-349). OCTAVE employs a three-phase approach that is founded on information asset identification and valuation. In Phase 1, the focus is on defining, documenting, and valuating critical information assets within the organization. Asset profiles are created, documenting the critical information assets on which the organization relies. These profiles record the information asset's value, owners, required security controls, threats and vulnerabilities, and other critical constructs of the information asset. Technological vulnerabilities within the infrastructure are not documented until Phase 2. In Phase 3, risk is analyzed and security plans, policy, and other controls are created and employed to mitigate the risk (Alberts and Dorofee 2001, pp. D-19-21). Because of its focus on the identification, documentation, and valuation of information assets and technology, OCTAVE is a comprehensive risk management approach that lays a solid foundation for CDA-D/MIA framework implementation.

Air Force Operational Risk Management Program.

The Air Force employs a risk management program entitled the Operational Risk Management Program (ORM) (AFPD 90-9 2000; AFI 90-901 2001). Among the primary goals of ORM are enhancement of mission effectiveness at all levels, while protecting the organization's assets and improving war fighting mission effectiveness and mission accomplishment (AFPD 90-9 2000). Air Force Instruction (AFI) 90-901 (2001) implements the ORM program and correctly identifies the critical risk management steps of identification, assessment, and control of risk to operational assets. However, it is important to note that the ORM process does not explicitly recognize cyber information

assets in its assessment process. Air Force ORM deals exclusively with risk management of physical assets.

Section Summary.

An effective risk management is critical to establishing an effective information security program. There exist distinct differences in the approaches to risk management, so an organization must carefully choose one the enables a comprehensive approach to effective information protection. Many organizations do not perform effective risk management activities, or limit the scope of the risk management functions such that they are ineffective. An asset-focused approach that enables identification and valuation of the information assets on which the organization depends, and identifies the business processes and goals which they support, such as the OCTAVE approach (Alberts, Dorofee et Al. 2003), is essential to building the foundation of defensive cyber damage assessment.

Information Assets

This section will examine the relevance of information as an asset to the organization. As Drucker (1995) correctly recognizes, information is the center of gravity for daily operations within the modern business organization. This dependence exists because information holds relevance and value as knowledge to the organization. The distinction between information and the IT that enables organizations to effectively use it is often blurred. Understanding this distinction is fundamental to creating an approach to cyber security that facilitates defensive cyber damage assessment. This

section examines literature that provides a fundamental understanding of information as an asset.

An Information Taxonomy.

This aspect of CDA-D/MIA development research is primarily concerned with developing an understanding of the difference between data and information. They are frequently confused and used incorrectly referred to interchangeably. Some communities of interest mistakenly hold that there is little distinguishable difference between, data, information, and knowledge (Alavi and Leidner 1999). However, a better understanding of each reveals the distinct contextual differences that define each and provide the foundations for information taxonomy. Data is the foundation of this taxonomy. The information taxonomy develops as information progresses from raw data to information to refined knowledge suitable for decision-making (Kanter 1999, pp. 8). The catalyst for development of the taxonomy is the assignment of contextual meaning through human application and utility (Petrocelli 2005, p. 181).

Data is the subset of information and the focus of traditional cyber security schemes that focus on the storage, access, and protection of the container system on which the data is stored. However, data has no inherent value. It is completely dependent upon its external application to produce value (Petrocelli 2005, pp. 180-181). Human utility drives organization and aggregation of data into usable groupings of contextual relationships that endow the data with relevance and purpose. Thus data becomes information which, by its nature, is inherently associated with meaning (Spiegler 2000, pp. 8-9). Information, not data, is the center of this taxonomy, as it is the basic unit that contributes to the development of knowledge for use in all forms of decision making.

Knowledge is information further aggregated into a more usable form that can be made actionable to provide value to the organizational mission (Kanter 1999, pp. 7-9; Vail 1999, pp. 16-17). The ensuing information taxonomy reflects the increasing value as information is transformed and used within the organization for decision making (Spiegler 2000, pp. 9-11). Because information is the core asset of cyberspace, it must be at the center of asset focused security planning and risk management if cyber damage assessment is to be possible.

Contextual Value of Information.

The classical economics theory of uncertainty holds that information cannot be valued like consumption good. Information is useful primarily as an input to decisions, and is extremely difficult to assign a quantitative value (Van Alstyne 1999, pp. 328-329). The value of information is dynamic and changes from one organization to the next; and even within an organization as the context that assigns value changes (Petrocelli 2005, pp. 185-189). This *problem* of context introduces a varying level of uncertainty in assigning value, and is one factor that has confounded many attempts at developing models to account for and definitively measure the value of an information asset (Soo Hoo 2000, p. 7). Information value is not static explicitly because of this concept of context. Its value is always relative to some target goal (Morrision and Cohen 2005, p. 34). If the information asset *aligns with* the mission by strongly supports an organization's strategic goal, the asset will prove to hold a high level of contextual value to the organization whole; especially if the asset is a direct contributor to some competitive advantage gained or held by the organization (Willcocks 2004, pp. 241-245). When the information asset directly aligns with the mission of the entire organization, its

contextual value is simple to understand. However, an asset may exist within the hierarchy of missions that exist within an organization. Determining the value of the asset may not be as readily determined without examining the assets utility in relation to its support for mission operational processes. However, it is important to realize that the primary value driver for information is externally determined by how the owner tied the information asset's usability to achieving some goal the owner desires (Buffett, Scott, et. Al. 2004, pp. 80-81; Morrison and Cohen 2005, p. 34).

Remember that Albert's hierarchy of missions says that an organization maintains an ordinal stacking of missions that work together to support the organization's established goals. Each organizational function has its own goals and processes that support is mission. This functional mission supports the organizational mission, in turn. Each of these functions depends on information assets and systems with an inherent contextual value to the respective function. An information asset that is critical to the mission of one function may have little or no value to another, but still have hold high value to the organizational mission. This supports Petrocelli's assertion the value of information is not static, but is a function of context and perspective relating to mission (Petrocelli 2005 pp. 183-184). Consider, however, that an information asset that is of high value to as supporting function within the organization can also be high value to the organization as a whole; depending on the degree of dependence of the organization's mission depends of the function's operational processes that rely upon that asset.

Information also holds contextual value that can change throughout its lifecycle. Information can age beyond usefulness. It can suffer compromise to its confidentiality,

availability, or integrity that may reduce its usefulness to the organization, which equates to degradation in value to the organization.

Owners, Custodians, and Consumers of Information Assets.

The traditional thought on information responsibility and usage hold that there are three basic categorical communities that "touch" information: information owners, information custodians, and information consumers, or users. It must be noted that there is no commonly agreed upon definition of any of these and that different communities of interest include additional, more specific categories. A commonly accepted definition for an information owner, however, is "the person or group responsible for applying security policies to an information object" (Computer Desktop Encyclopedia n.d.). Stephens states "owners of an information asset are those individuals who have primary responsibility for the viability and survivability of an asset" (Stevens 2005, p. 6). The information custodian is the individual or group of individuals within the organization that bears the responsibility for protection of the information asset as it is stored, moved, or processed. Owners are responsible for establishing the security requirements and custodians are responsible for ensuring the requirements are carried out. Stephens also states the information owner, not the custodian, is responsible for understanding the value that the asset maintains to the organization (2005, p. 7). The custodian, however, is responsible for the infrastructure in which the asset resides; and is responsible for no more than the protection and assurance activities required to keep the asset safe and accessible. According to Stephens (2005, p. 7), in many organizations the owner is unaware of his/her basic responsibilities and custodianship is frequently confused with ownership.

The information user, or consumer, depends upon the information for some process, but does not necessarily bear ownership or custodial responsibilities. This definition does not preclude the consumer from bearing any responsibility for protecting the information. The consumer is most often closest to the asset and associated risk (Spears 2006). For this reason, the consumer must bear some degree of custodial responsibility when using information. Stephens illustrates this with a scenario of a user accessing a database from a desktop.

> "In essence, the user, as the manager of that desktop, is temporarily also a custodian. Custodians are generally required to provide due care over the information asset while it is in their possession. Thus, the user should ensure that she protects this information asset as well as or better than it was protected at the container from which she received it. More importantly, the user should protect the information asset commensurate with its security requirements. If she cannot, the owner of the information asset should deny her access to it or deny her the privilege of acting as a custodian for the information. (Stevens 2005, p. 8)"

It is important to understand that these three categorical communities of information responsibility are not mutually exclusive. An information owner can also be the custodian, with responsibility of determining value and security controls for an information asset, and responsibility for the technological asset that contains the information asset. As this literature has shown that the user can bear some degree of custodial responsibility, the owner can also be any one of many consumers. Stephens observes that in the real world, an information asset may have multiple owners, and thus, many different security requirements. This is an important concept to understand when attempting to determine damage caused to an information asset by a successful cyber attack.

Information Assets vs. Information Technology Assets.

Operations rely on information, and this research has established that modern organizations rely largely upon information in cyberspace. Because of this dependency upon specific information, operations regard the information on which it depends as an asset. Information technology is an *enabler* for operations to achieve improved access to that information. Consider that in IT non-availability, it is conceivable that operations can continue if another mode of information delivery is contrived. However, with the scenario reversed, the presence of IT would not enable the mission without the information asset on which the mission depends. In his controversial article, *IT doesn't matter* (Carr 2003, p. 41-42), Carr hits precisely upon this issue. Too many organizations erroneously believe that IT will provide a competitive advantage and focus on IT as a vehicle to strategic success. Carr correctly argues that IT offers no such guarantee (2003, pp. 41-43). Carr's stance supports Davenport's assertion made earlier in this literature review that technology is not an equitable substitute for information (Davenport and Prusack 1998).

An exclusive focus on IT is especially dangerous when attempting to establish an effective security program. The first step of such a program must identify what must be protected. If the focus is exclusively on a single target asset group, developing a comprehensive understanding of the value and potential impact from risk realized becomes difficult. (Soo Hoo 2000, pp. 10-11). By first understanding and identifying information as an asset, followed by understanding the its relationship with it technological container, a more comprehensive approach to setting security controls can be established..

Valuation of Information Assets.

Information and the systems that contain and process it are among the most valuable assets of any organization (GAO 2000, p. 2). Virtually all existing literature regarding data, information, or knowledge value attempts to assign economic value to the asset. This is not surprising, since the vast majority of the available work is sponsored by for-profit private sector organizations. It is important to realize that the common thread is that information assets are not purely commodities with prefixed value. The way information is valued varies in a large degree on the perspective of the *information owner* (Buffett, Scott, et. Al. 2004, p. 79). It must be recognized, however, that the primary value driver for information is not internal. The value of information is determined by how it can be used by its owner and this value is necessarily tied the utility in achieving some goal the owner desires (Buffett, Scott, et. Al. 2004, pp. 80-81; Morrison and Cohen 2005, p. 34). Therefore, any valuation of information must reflect this acknowledgement of utility as a value driver for the valuation to be meaningful to the owner.

Section Summary.

This section examined literature fundamental to establishing the concept of information as an asset within the modern organization. Organizations depend on information to accomplish the mission. Technology enables the flow of and access to the information. Data has no inherent value, about must be organized in such a way that it becomes information and gains meaning and, thus, value to the organization. The information asset has owners, custodians, and consumers that hold differing perspectives of the information, respectively. Information is frequently forgotten when exclusive focus is placed on the technology that supports it. This limits the understanding of the

value the information holds to these communities of interest and the organization as a whole. Information, not technology, must be viewed as the chief asset in an information organization if value is to be realized. Only then can damage and mission impact assessment be fully realized.

Relevant Laws, Orders, Doctrine and Guidance Relevant to Cyberspace

A large body of law, directive, and guidance exists to govern the conduct of the various aspects of military and government operations in cyberspace. This section will take a comprehensive approach to provide an exhaustive review of the literature and law applicable to conduct of cyberwarfare and the establishment of a defensive cyber damage assessment framework.

Legal Implications of Cyberwarfare.

Air Force Policy Directive 51-4 (1993) mandates that Air Force personnel are required to comply with the Law of Armed Conflict (LOAC) while engaging in armed conflict. It defines armed conflict is defined as a situation where at least one state has engaged in use of armed force (1993). There exists much debate about the legality of offensive cyberwarfare operations and what, in cyberspace, equates to an armed attack. The Air Force is keenly aware of this and addresses this subject in AFDD 2-5, *Information Operations* doctrine. Dr. Thomas Wingfield addresses this issue through review of international law. He reports that the Charter of the United Nations articulates the principle of *jus ad bellum*, which is "the portion of international law that governs the lawful resort to force (Wingfield 2006, p. 2)." Wingfield determines that there are many issues when defining the threshold of escalation from cyber conflict to the equivalent of

armed conflict. One of the many concerns raised in other literature is the issue of collateral damage which may have unexpected affects on unintended targets. Collateral damage is a concern in the cyber domain because of the many interdependencies upon information assets. Cyber attacks are not bound by the laws of physics and the effects of an attack may have unintended consequences on the other side of the world. Failure to accurately assess the collateral damage of a cyber attack may be unethical at best, and illegal at worst (Rowe 2005). Ultimately, however, Wingfield concedes that there is still no consensus on the legality of cyber warfare (Wingfield 2006, pp. 12-13).

DiCenso comes to a similar conclusion by pointing out that no clear guidance exists to define what constitutes armed force (DiCenso 1999, p. 88). DiCenso holds The Air Force's definition of a weapon (AFI 51-04 1994) clearly indicates that there does not appear to be any legal issue of significance regarding the application of cyberwar in regards to LOAC. The areas of cryptology and encryption have raised much interesting discussion regarding this, but primarily concerning policy and strategy rather than legality. Both Wingfield and DiCenso agree that current interpretation of international law holds that a nation allows a nation to engage in defensive cyberwarfare operations to protect its cyber and real-world assets in any way, so long as these activities do not negatively impact another nation's assets (DiCenso 1999 pp. 98-99; Wingfield 2006, p. 12).

Doctrine on Information Operations and Cyberspace.

In 2006, both the Chairman of the Joint Chiefs of Staff (CJCS) and the United States Air Force issued revised joint doctrine on Information Operations. The DoD's standard for military terms, Joint Publication (JP) 1-02 (2006), was also updated to reflect

these changes. Prior to this revision, both doctrinal documents made a clear delineation between offensive and defensive activities in Information Operations (IO). This recent update to JP 3-13, Information Operations (2006) states that Joint IO doctrine now "discontinues use of the terms 'offensive IO' and 'defensive IO'", but states that "the recognition that IO is applied to achieve both offensive and defensive objectives (JP 3-13 2006). " This revised joint doctrine places computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE) functions under one umbrella by establishing Computer Network Operations (CNO). JP 3-13 cites CNO as one of the five core capabilities of joint IO doctrine (JP 3-13 2006). The following table displays the notional revision of joint IO structure (see Table 2 below). It is worthy to note that the term information warfare is no longer used in joint doctrine.

Table 2. Information Operations Integration into Joint Operations

INFORMATION OPERATIONS INTEGRATION INTO JOINT OPERATIONS (NOTIONAL)						
Core, Supporting, Related Information Activities	Activities	Audience/ Target	Objective	Information Quality	Primary Planning/ Integration Process	Who does it?
Electronic Warfare	Electronic Attack	Physical, Informational	Destroy, Disrupt, Delay	Usability	Joint Operation Planning and Execution System (JOPES)/ Targeting Process	Individuals, Governments, Militaries
	Electronic Protection	Physical	Protect the Use of Electro-magnetic Spectrum	Security	JOPES/Defense Planning	Individuals, Businesses, Governments, Militaries
	Electronic Warfare Support	Physical	Identify and Locate Threats	Usability	Joint Intelligence Preparation of the Battlespace(JIPB)/SIGINT Collection	Militaries
Computer Network Operations	Computer Network Attack	Physical, Informational	Destroy, Disrupt, Delay	Security	JIPB/JOPES/Targeting Process	Individuals, Governments, Militaries
	Computer Network Defense	Physical, Informational	Protect Computer Networks	Security	JOPES/J-6 Vulnerability Analysis	Individuals, Businesses, Governments, Militaries
	Computer Network Exploitation	Informational	Gain Information From and About Computers and Computer Networks	Security	JIPB/Targeting Process	Individuals, Governments, Militaries
Psychological Operations	Psychological Operations	Cognitive	Influence	Relevance	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Military Deception	Military Deception	Cognitive	Mislead	Accuracy	JOPES/Joint Operation Planning	Militaries
Operations Security	Operations Security	Cognitive	Deny	Security	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Supporting Capabilities	Information Assurance	Informational	Protect Information and Informatin Systems	Security	JOPES/J-6 Vulnerability Analysis	Businesses, Governments, Militaries
	Physical Security	Physical	Secure Information and Information Infrastructure	Usability	JOPES/Defense Planning	Businesses, Governments, Militaries
	Physical Attack	Physical	Destroy, Disrupt	Usability	JOPES/Joint Operation Planning	Governments, Militaries
	Counterintelligence	Cognitive	Mislead	Accuracy	JIPB/Human Intelligence Collection	Governments, Militaries
	Combat Camera	Physical	Inform/Document	Usability, Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
Related Capabilities	Civil Military Operations	Cognitive	Influence	Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
	Public Affairs	Cognitive	Inform	Accuracy	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
	Public Diplomacy	Cognitive	Inform	Accuracy	Interagency Coordination	Governments

(JP 3-13 2006)

The Air Force (AFDD2-5 2005) has created a network operations capability which is comprised of three functions mirroring the joint CNO construct. The Air Force's Network Warfare operations (NW Ops) are the integration of the military capabilities of network attack (NetA), network defense (NetD), and network warfare support (NS). The intent of NetA is to perform offensive operations against the adversary's cyber information assets with the desired effect of "influence[ing] the adversary commander's decisions. (AFDD2-5 2005)" In this way, Air Force IO doctrine acknowledges that cyber operations can impact the adversary's mission capability, both in the cyber domain and in real world operations.

Federal Information Security Act of 2002 (P.L. 107-347, Title III).

The federal government has a limited role in the overall security of the national infrastructure. The Department of Homeland Security (DHS) is the federal government's primary agent for working with state and local governments, the private sector, academia, and the general public to ensure necessary measures are enacted to protect the national information infrastructure (Moteff 2004). It has, however, produced requirements for securing those information systems under federal control through the passage of P.L. 107-347, Title III, commonly known as the Federal Information Security Act *(FISMA)* of 2002 (United States Congress 2002). FISMA recognizes that the chief underlying factor in the majority of information security problems within federal agencies this the employment of an ineffective information security program; and attempts to create a comprehensive framework for more effective information security (GAO 2005). FISMA authorizes the National Institute of Standards and Technology (NIST) to develop the security standards and guidelines that will be used on federally "owned" *non-national security systems*. Section 3542, subparagraph (2A) defines a *national security system* as any computer or telecommunications system that is operated by a federal agency, or agency contractor, and used in a function or activity which:

- Involves intelligence activities;
- Involves cryptological activities related to national security;
- Involves command and control of military forces;
- Involves equipment that is an integral part of a weapon or weapons system;
- is critical to the direct fulfillment of military or intelligence missions; or
- "is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be dept classified in the interest of national defense or foreign policy (United States Congress 2002)."

Subparagraph 2B explicitly excludes systems that meet the above criteria, but are "used for routine administration and business applications *(including payroll, finance, logistics, and personnel management applications)* (2002)."

Of particular interest to this research is the requirement throughout FISMA to provide an information security program commensurate with amount of potential damage that could result from a successful compromise. Furthermore, FISMA specifically cites the information stored on the system, rather than the information system exclusively. Section 3544, subparagraphs (2)(A-D) specifically tasks the head of each agency under the authority of FISMA to ensure senior agency officials establish an information security program based on risk to the *assets that support operations*. This is extremely important as it implies the need for asset-focused risk assessment, which is the foundation of defensive damage assessment. Section 3544, subparagraphs (2)(A-D) reads as follows:

> ‘‘’(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—
>
> ‘(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;
>
> ‘(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;
>
> ‘(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and
>
> ‘(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented; (United States Congress 2002)"

National Security Directive 42 (NSD-42).

NSD-42 (Bush 1990) describes the foundational goals for information technology and telecommunications security within the federal government and provides basic implementation strategy for securing the systems designated as national security systems. This directive mandates the national security telecommunications and information technology must be reliable, effective, efficient, and have a sound technical base. NSD-42 was signed by President George H. Bush on July 5, 1990. NSD-42 explicitly names the Director, National Security Agency (NSA) as the National Manager for National Security Telecommunications and Information. Among the many authorities granted to the National Manager is the responsibility to assess the overall security posture, to include threats and vulnerabilities to national security systems. The contextual support provided by the other Directives and Orders examined in this section support the assumption that the intent is to protect the information procession systems and the information assets residing on these systems.

HSPD-7 and the President's National Strategy to Secure Cyberspace.

The Homeland Security Presidential Directive No. 7 (HSPD-7) is an extension of basic policy established by the previous administration's Presidential Decision Directive No. 63, and states that is the United States policy to enhance the protection of the nation's critical infrastructure. HSPD-7 is inclusive of both cyber and real-world infrastructure assets, but specifically directs the Secretary of Homeland Security to maintain and organization that serves as the cyber security focal point by coordinating protection efforts between public and private sector and academia (Bush 2003).

According to John Moteff (2004), *the President's National Strategy to Secure Cyberspace (PNSSC)* (NIAC 2002)carries less weight than public law or presidential directive, it is still considered an important step towards bringing together all interested parties in securing those mission systems and processes dependent on cyberspace (Moteff 2004). The PNSSC outlines the strategic importance and strategic objectives for protecting cyberspace-dependent systems and operations. This document supports, and at times overlaps, other Executive Orders and Presidential Directives and recommends specific tasks which include vulnerability threat and warning sharing, integrated exercises to test cyber security response and effectiveness, coordination of national threat assessment.

The recommendations PNSSC makes are only guidelines for suggested implementation. Many experts feel that this plan falls short of its intended purpose. In 2004, the Professionals for Cyberspace Defense, an elite group of approximately 40 concerned scientists and cyber security experts (PCD 2002b), expressed concern that no definitive research or validation had been conducted to assess the national vulnerability to date. The PCD cited a "failure to establish the full nature of the problem represents a fundamental flaw in the White House strategy (Saydjari 2002, p. 125)."

CJCSM 6510.01 Ch 3 ANNEX A TO APPENDIX B, ENCLOSURE B.

Chairman of the Joint Chiefs of Staff Manual (CJCSM) No. 6510.01 Change 3, *Defense-In-Depth: Information Assurance (IA) And Computer Network Defense* (CND), 08 March, 2006 is a limited distribution document, therefore only a very specific section of this manual that is very important to this research will be discussed. CJCSM 6510.10 Ch3 Annex A to Appendix B to Enclosure B establishes the responsibilities of the Joint

Staff, combatant commands, Services, Defense agencies, DoD field activities and join activities. This manual very explicitly prescribes the *operational impact assessment* resulting from a successful cyber attack on DoD networks be provided to commanders and other responsible communities of interest (CJCSM6510.01 2006). To meet this requirement, a validated defensive cyber damage assessment framework *must* be in place to provide commanders and other required personnel with timely and accurate operational impact report. Without a validated framework, cyber damage assessment is a non-standardized, undependable estimate of the damage caused by cyberspace incidents on Air Force networks (Thiem 2005, p. 43).

Air Force Instruction (AFI) 10-206 Operational Reporting.

AFI 10-206 *Operational Reporting* establishes the Air Force Operational Reporting System (AFOREPS) and the Operational Status Event/Incident Report (OPREP-3). AFOREPS is a set of reports intended to provide Air Force level leadership and intermediate commands with timely situational awareness information to make timely operational decisions. The OPREP-3 is one of the key reports that contribute to the AFOREPS. The OPREP-3 report is an immediate report issued to notify commanders of any significant event or incident that effects MAJCOM, HQ USAF, or DoD mission; to include events that impacts the commander's mission capability in such a way that higher level mission is affected (AFI 10-206 2004). The OPREP-3 report categorizes events and incidents according to their potential impact. AFI 10-206 explicitly defines the criteria for each various types of OPREP-3 reports, and more importantly the report content and reporting procedures for each. This AFI establishes the mechanism for up-channeling incidents that impact an organizations mission capability; and therefore is

important guidance for establishing initial mission impact reporting following cyber damage assessment.

AFI 33-138 Enterprise Network Operations Notification and Tracking.

AFI 33-138, *Enterprise Network Operations Notification and Tracking* establishes a hierarchy of reporting for all issues and incidents occurring on Air Force networks. It implements, among other guidance, the incident and vulnerability reporting requirements specified in CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense* (2006). This AFI prescribes and explains the various notification and tracking processes required to direct and coordinate action and report status within the Air Force Network Operations (AFNETOPS) hierarchy.

AFI 33-138 (2004) is establishes a unified and standardized reporting system that facilitates rapid dissemination of incident notification and the command and control direction for response actions throughout Air Force networks. Specifically defined in this AFI are the reporting and directive actions required for such protective and preventive activities network security incidents reporting, Time Compliance Technical Orders, and Classified Message Incidents. The reporting structure established by this AFI is especially well suited for rapid multidirectional information dissemination through the AFNETOPS command and control structure to the information owners affected by a successful cyber attack. The unified and consolidated incident reporting structure established by this AFI is very important to ensuring the rapid and secure damage assessment reporting information to both AFNETOPS command and control, and potentially affected information owners.

Section Summary.

This section considered the body of essential laws, directives, doctrine, and service instructions that provide guidance for the conduct of cyberspace and cyberwar operations, and the establishment of a defensive cyber damage assessment framework; and established that there are few legal complications associated with defensive cyberwarfare activities. Particularly noteworthy is FISMA's requirement that agencies under its jurisdiction establish security controls for both operations and assets that is commensurate with amount of potential damage that could result from a successful compromise. This wording strongly implies asset-focused risk management, which is the foundation for an effective CDA-D/MIA framework. Although FISMA does not apply to national security systems, commanders responsible for systems supporting military operations under CJCSM 6510.01 Ch 3 are required to provide operational impact assessment following a cyber security incident. AFI 10-206 Operational Reporting and AFI 22-138 establish operational impact reporting requirements and establish a unified reporting system on Air Force networks.

Related Research and Work

This research has stated that the financial loss estimation desired by for profit organizations provide a less effective decision making tool for non-profit driven institutions such as the military. This statement is true when considering the necessary decision input for tactical and operational decisions. In strategic decision making, however, the military shares a common interest with the profit driven sector. As shrinking budgets and an important war on terror cause DoD leadership to carefully

guard every dollar spent; wise investment in information technology and the security controls to protect the information assets within becomes highly important. In this context, understanding the financial losses caused by successful cyber security incidents has value for making important long-range decisions.

Determining Large Scale Economic Loss.

Damage assessment models that fit a military decision making framework are scarce. In relative contrast, models that seek to determine the economic loss caused by a successful cyber attack seem to abound. If a model is to describe financial lose within and organization, such as the military, it must be able to address the effects of large scale attack distributed across a wide area. One approach is to attempt assessment of large scale economic loss of time (Dubendorfer 2004). The Dubendorfer, et. Al., scenario assumes an external attack via the Internet. This attack specifically launches a dedicated denial of service (DDoS) attack against national infrastructure provider in an attempt to severely degrade wide area service and negatively impact companies. This scenario further assumes that the attack has a relatively short duration, measured in hours to days. The attacker's expectancy is that a significant degradation in Internet performance will result in financial loss and that the longer an attack lasts, the greater the potential economic impact (Dubendorfer 2004). Furthermore, economic impact can increase past the duration of the attack, unlike technical impact, which generally ends with post-attack remediation.

The Dubendorfer, et. Al. model approaches this duration of potential economic impact as $t \to \infty$, where $t = t_0$ is the time of the attack start, and $t = t_1$ as the time of attack completion. The interval following the attack is represented as $[t_1, t_2]$, where t_2

presumably represents completion of remediation and return to normal business. Duration of impact beyond t_2 is represented as $t > t_2$.

This model attempts to estimate economic loss within categories of types of damage. Dubendorfer, et. Al, identify the following four categories:

1. *Downtime Loss*: Total downtime loss (L_D) is comprised of two subcategories, productivity loss, where the incident forces employees to utilize less efficient means of accomplishing assigned tasks, and revenue loss. Downtime loss may be represented as the sum of these two; and may be modeled as follows: $L_D = \frac{E_{ca}}{d_a} \cdot d_0 \cdot E_{no} \cdot E_{po} + \frac{R_a}{ds_a} \cdot ds_0 \cdot R_0 \cdot S_0$, where E_{ca} represents annual cost per employee, d_a represents working time per employee per year, d_0 represents working hours overlapping outage time, E_{no} represents the number of employees affected, E_{po} represents productivity degradation during the incident, R_a is the total annual revenue, d_{sa} represents annual service operating hours, d_{so} represents service hours affected by outage, R_0 represents that part of revenue affected by the outage, and S_0 represents the degree of service degradation (Dubendorfer 2004)
2. Disaster Recovery: Disaster recovery costs L_r include the time, material and additional incidental expenses incurred for restoration and recovery following an incident. Disaster recovery costs may be modeled as the sum of costs incurred during downtime, cited by Duberdorfer, et. Al., as $[t_0, t_1]$. It is

modeled as: $L_r = E_r \cdot E_{ch} \cdot d_r \cdot + M_c$, where E_r represents number of employees assigned to recovery team, E_{ch} represents hourly cost per team member, d_r represents non-"duty" hours work, and M_c represents material costs incurred (Dubendorfer 2004).

3. Liability: In some cases the incident may result in the organization failing to fulfill contractual obligations with third party organizations. These organizations may demand financial compensation, resulting in liability costs (L_c). Liability costs may modeled as follows: $Lc = \sum C_C + \sum C_l$, where $\sum C_C$ represents the sum of all compensation claims, and $\sum C_l$ represents the sum of all liability claims (Dubendorfer 2004).
4. Customer Loss: The incident may result in loss of customers, depending on various factors. The impact of customer loss cost (L_{CL}) may accrue for a long time, and potentially have a negative on recruitment of new customers. This long-term loss may be modeled by considering sum of actual customers (C_A) and potential customers lost (C_P) over time (Δt), multiplied by the average revenue per customer (R_C) and follows: $L_{CL} = [C_A(\Delta t) + C_P(\Delta t)] \cdot R_C(\Delta t)$. Dubendorfer further notes that if R_C has a high variance, this model is inaccurate. When this occurs, a detailed analysis should be used, representing only the critical customers (Dubendorfer 2004).

It should be noted that this type of model may be suited specific non-operational, strategic decisions that military decision makers consider when determining budgetary IT

issues, such as level of investment in technological security controls. Such a model can perform suitably for assessment of economic loss. Associating the information's value with an economic handle provides some tangibility to the information, but still cannot the intangible property of utility. Development of such a model would provide some benefit to the decision maker of an organization not driven by economic profit motives.

A Utility-Based Value Model for Information Decision Making.

This section will briefly discuss the concepts of another model (Morrison and Cohen 2005) that information value from a utility-based perspective. This model focuses on the value of information being relative to some goal decision (Morrison and Cohen p. 34). This has important implications about developing value handles for the intangible properties by which information presents value to the organizations.

Morrison and Cohen present their base target decision model (p. 35, eq. 1) as a way to model simple decision making based, where the target hypothesis relates to the utility value of information. This model is explicitly geared towards making economic based decisions based on , so no further discussion will entail about the details of the model. The model is noteworthy, however since it provides one way to determine relative value through the information utility.

Damage Assessment on Air Force Networks.

Case study research (Thiem 2005) conducted to understand how defensive damage assessment was being conducted on Air Force networks focused on information collected through interviews with subjects working in MAJCOM NOSCs and the Air Force Computer Emergency Response Team, now renamed AFNOSC NSD (AFI 33-138 2004). This effort established that some degree of damage assessment is attempted in

various places within the Air Force networks. However, Thiem cites that "individual organizations within the [Air Force] are developing their own methods and models to perform network damage assessment (Thiem 2005, p. 43)." The research notes that several of the assessment methodologies discussed did not apply guidance, such as AFI 10-206 (2004) to ensure that impact to mission capability was considered in the assessment. Without an established standard and validated methodology, cyber damage assessment on Air Force networks is unreliable at best.

Two interesting concepts are uncovered by Thiem's research that underscore topics previously discussed in this chapter and are worthy of further examination. First, it is noteworthy that one of the few commonalities between damage assessment methodologies was the focus on damage to the system. Two respondents to the survey answered that damage assessment is unnecessary since it takes focus away from infrastructure protection. Clearly, this response is symptomatic of the limited scope of understanding created by technologically focused scenario analysis approach to risk management discussed by Soo Hoo (2000, p. 11). This mindset, as reflected by the respondents, holds protection of technology at a higher priority than protection the information asset itself. This disregard for the technological enabler over the mission critical asset causes problems on many levels and may be indicative of a perspective that may be preventing effective and accurate damage and mission impact assessment on Air Force networks.

Secondly, not a single respondent addresses the issue of mission capability impact that may result from a successful cyber attack. Impact analysis, a predictive estimation of damage to the operational mission if an asset is lost, is not considered (Stoneburner,

Goguen, et. Al. 2002, p. 12). The survey interviews conducted by Thiem (2005) shed light on several problematic issues regarding the current status of damage assessment on Air Force networks, and problems that may be preventing effective damage assessment and mission capability assessment being implemented under the existing approach to network security and risk management.

The Horony Damage Assessment Model.

Research (Horony 1999) conducted at the Air Force Institute of Technology aimed to develop a model for Information System damage assessment. This research was exploratory and the model produced conceptual. Horony identifies eight primary factors he states an Information Systems manager should consider during the risk assessment process. The eight factors of the Horony model (see Figure 6 below) are:

- Recovery
- Data
- Education/Training
- Lost Revenue
- Business Expenses
- Reputation
- Productivity
- Human Life.

Horony breaks down each of these categories, or *factors*, into *sub-factors.*

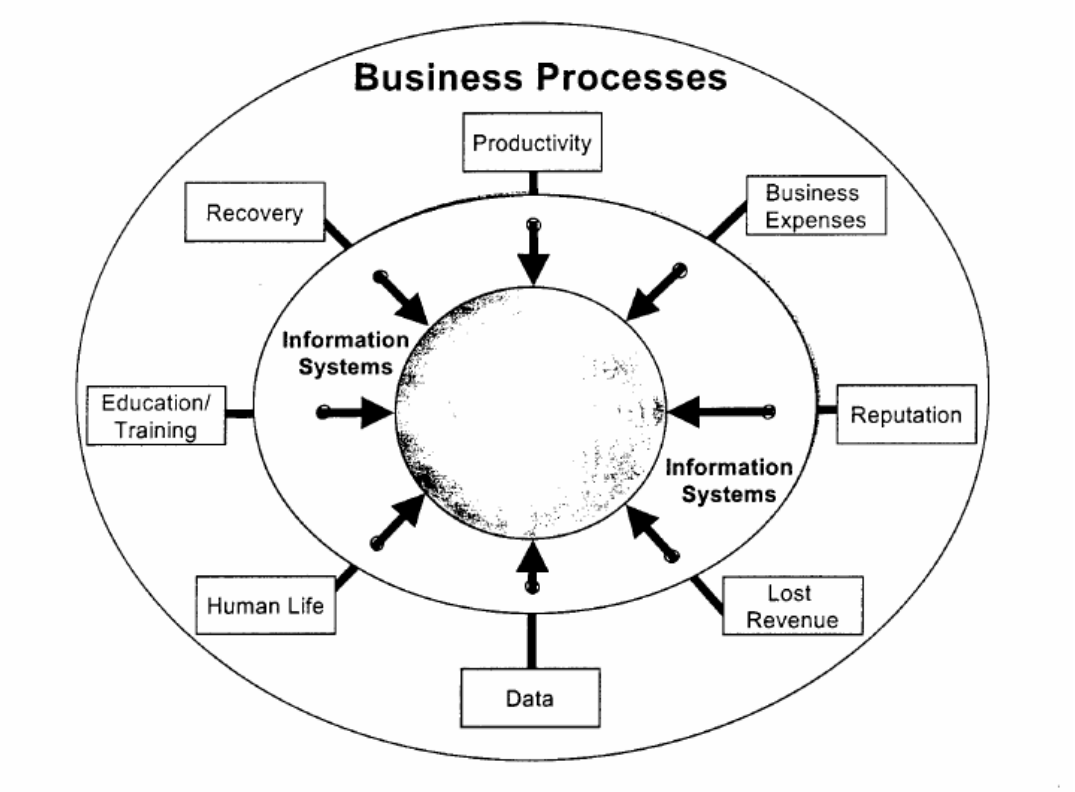


Figure 6. Horony Damage Assessment Model (1999, p. 35)

The Recovery Factor.

Horony defines recovery as the "process that system administrator must take to restore an information system to the most current state prior to the incident (Horony 2000, p. 30)." Under this definition, the recovery factor of the Horony model includes all those activities involved with incident response, investigation, and remediation.

Horony defines five sub-factors as subsets of the recovery factor. These are *investigation, restore, software / hardware, consultants / contractors,* and *accounts.* The *investigation sub-factor* consists of all activities undertaken to determine incident causality and consequential damage incurred. Horony includes such things as intrusion detection, determining the damage, incident handling under this sub-factor (Horony 1999,

p. 37). The *restore sub-factor* includes all infrastructure affected by the incident. Infrastructure items, such as servers, routers, bridges, gateways, desktop systems, etc. must be returned to the pre-incident state through means such as backup restoration, system rebuild, or purchase. The *software /hardware* sub factor considers damage or loss to infrastructure system software or infrastructure system component hardware that would require replacement. Horony states that this could include hardware or software confiscated by an authorized investigative agency and any hardware or software deemed necessary to improve system security (1999, p.37). The *consultant / contractor sub-factor* consists of any outsourcing of manpower for assistance in investigative and/or recovery activities. Such activities could include use of clean-room facilities for forensic investigation, or specialized data recover assistance from damaged storage media. The *accounts sub-factor* address actions required to bring affected accounts back online, providing users access to the IS systems, once available.

The Education/ Training Factor.

The second primary factor of the Horony model is Education / Training. Horony states that "as an investigation proceeds the need for additional education and training within the organization may become evident. Systems administrator and information security personnel may not have the necessary skill to perform a thorough investigation (Horony 1999, p.31)." Therefore, this model takes into account the cost associated with providing training to organization personnel following an incident.

The constructs of the *Education/Training* factor are *System Administrator/Information Security Personnel* and *Employee COMSEC/INFOSEC.* The *System Administrator/Information Security Personnel sub-factor* covers training for those

personnel with IS administration or security responsibilities. The *Employee COMSEC / INFOSEC* covers training for system users. Horony specifically identifies training on user security policy such as password security, system security and other issues normally covered by the normal security training program (1999, p.38).

The Business Expenses Factor.

The third primary factor is Business Expenses, which are defined all the direct business costs resulting from the incident. This factor attempts to measure the impact of lost systems that affect both internal and business-to-business processes. Only a small number of respondents to Horony's survey agreed that business expenses are a useful part of damage assessment. The sub-factors of this primary factor are *Customer Service* and *Business to Business.* The *Customer Service sub-factor* attempts to factor in such costs as those associated with paying "late fees, overdraft fees, and other fees associated with accounts affected by a system outage (Horony 1999, p.31). *The Business to Business* sub-factor attempts to capture the effect the incident had on the organization's critical inter-business relationships on which the organization depends, such as the failure of a Just-in-Time inventory system.

The Productivity Factor.

This factor attempts to measure the impact an incident has on an organizations production costs. When an incident occurs, the system or systems affected by the incident will, be affected, in turn, affecting productivity. This factor is comprised of three sub-factors, *Mission Impact*, *Downtime*, and *Communication*. The *Mission Impact sub-factor* prescribes measurement of an organization's ability to maintain normal levels of productivity in its business processes. For a military organization, this may be a

measurement of sorties launched. For a corporate organization, this may be a measurement of any change in assembly line production. The Downtime sub-factor prescribes measurement *mission stoppage* resulting from an incident. The Communication sub-factor prescribes measurement of the effect the incident had on the *communication* infrastructure.

The *Productivity* factor addresses extremely important constructs for information damage assessment, but unfortunately falls short of the mark in terms of implementation ability. Horony prescribes measurement, but doest not propose how these items may be measured. An examination of this primary factor in relation to its sub-factors creates the basis for the argument that Horony should have actually entitled the primary factor Mission Impact, with the sub-components changed, accordingly.

The Data Factor.

The fifth primary factor is Data. Horony cites all respondents as identifying data loss as an important part of a damage assessment model (1999, p.32). The Data factor is comprised of the four following sub-factors: *Restoring, Re-Entering, Unrecoverable Data*, and *Proprietary Data*. The first and second sub-factors, *Restoring* and *Re-Entering*, appear to be related, although Horony does not explicitly state this. *Restoring* is defined as those activities involved with restoration of data from backup media, while Re-Entering encompasses those activities involved with manually inputting data that could not be restored from backup. The manner in which Horony describes these sub-factors presents a formidable challenge for implementation in an operational model. Although each is an important construct for measurement, it is arguable that it is in appropriate to include these sub-factors as measurements of impact to data. It seems

more logical to include these under Recovery costs. The third and fourth sub-factors, Unrecoverable Data and Proprietary Data, prescribe measurement of data that has been lost or compromised, respectively. These two sub-factors are certainly important to any user of a DAM attempting to determine post-incident damage

The Lost Revenue Factor

This factor prescribes measurement of revenue lost due to an IS incident. An IS incident may negatively affect an organization's ability to generate revenue by damaging otherwise impairing the organization's information systems associated with critical business processes. Horony lists two sub-factors belonging to Lost Revenue. These are Lost Sales and Lost Customers. The Lost Sales sub-factor prescribes measuring the impact, real or potential, on sales. The Lost Customers sub-factor creates a measurement requirement for determining customer loss

The Reputation Factor.

Horony reports that only five of the twelve respondents were felt that reputation was an important factor for damage assessment (1999, p. 33). It is important to note his citation that military respondents "were not overly concerned with reputation from the public's view point; however, they did concern themselves with how they were viewed by other military organizations (Horony 1999, p. 33)." Horony found that most, but not all, commercial organizations were interested in the post-incident affects on reputation. Reputation as a model primary factor is comprised of two sub-factors, Consumer/Public Confidence and Quality Employees. Horony states that organizational reputation relatively volatile and easily damaged (1999, p. 40). The Consumer/Public Confidence sub-factor attempts to capture this affect. While it may be argued that reputation may be

more resilient than Horony states, it is certainly true that once reputation has shifted negatively, it is both difficult and expensive to return to the previous states. A collateral effect of negative reputation may be that a company with a poor reputation may have difficulty attracting quality employees, which may result in additional problems for the organization. Horony attempts to capture this effect with the Quality Employees construct. The relevance of this as a viable metric for damage assessment in military operations is debatable.

The Human Life Factor

The final primary factor of the Horony model is *Human Life*. Loss of life is a serious concern for any organization, but especially military and other public service organizations in which an incident potentially could jeopardize human safety. The military is an obvious example, but such public and private organizations associated with such public services as police, fire, and transportation must also consider this factor. Horony includes two factors, *Loss of Life* and *High work load of ERT members*. The former prescribes measurement of the increased risk of loss of life following an incident. The latter prescribes a metric to determine the long-term stress effects on Emergency Response Team (ERT) members "causing undue stress and hardship on families (Horony 1999, p. 40).

The Horony model appears to be only one of a handful of attempts to develop a framework for assessing damage resulting from a successful cyber attack. It serves as an excellent foundation. Like other models, however, Horony's model attempts to assess economic loss. By doing so, the measurements are almost exclusively taken from the IT infrastructure that supports the information; therefore the infrastructure becomes the

center of the model, diminishing its ability to assess asset value. The result is a damage assessment model that provides a framework for measuring damage to the information infrastructure constructs (training, human life, revenue, systems, etc.), but yields little indication as to the extent of damage done to the information itself. This model lacks the critical measurement of *devaluation of the information* resulting from the incident. Information usability is a function of the value of information to the organization.

Several of the primary factors, and/or their associated sub-factors, in the Horony model have questionable application to military operations, and indeed any organization seeking to understand damage and impact to mission operations following a cyber incident. Many of the constructs have strategic use, but little immediate relevance in the tactical and operational mission domains. Consider for example the primary factor, *Education/Training.* Horony states that it may be necessary to provide training to administrators, InfoSec personnel, and users post-incident to ensure they understand system security issues and have required skills to prevent re-occurrence of such an incident. While it is true that some organizations may retain employees who require training to effectively perform their required duties, the organization's Security Education, Training, and Awareness (SETA) program must address this requirement. The SETA program is an integral and perpetual component of an effective organizational security program (Whitman and Mattord 2004, pp. 20-21). Accordingly, a SETA program would likely fund both pre-incident and post-incident education and training. Any peripheral costs associated with improving or otherwise modifying the COMSEC or INFOSEC programs as a result of post-incident fallout would be absorbed by these programs. For this reason, measuring impact to education and training from an IS

incident will produce little, if any, useful information for the user of such a model, rendering this primary factor invalid as a damage assessment area of measurement. Another area of concern lies among the sub-factors under the *Recovery* primary factor. Specifically, using the sub-factor entitled *investigation* is a misnomer that may confuse IS manager attempting to collect damage assessment data for this sub-factor. As stated before, Horony describes this sub-factor as encompassing all those activities associated with detection, response, damage assessment, and forensic investigation. The concern is that IS managers may only consider the impact metrics associated with the forensic investigation. In fact, what Horony describes in this sub-factor covers five of the seven components of incident response; of which investigation activities comprise two of the components (Mandia, Prosise, et. Al 2003, pp. 12-15).

Horony's research may be the first attempt to assess damage to military networks. However, because it is primarily concerned with economic impact assessment resulting from a cyber incident it can only offer very limited contributions to decision making in military operations. However, this model offers some utility in helping decision makers in the strategic domain understand the economic and human costs of cyber incidents on Air Force networks.

NIST Best Practices.

The National Institute of Standards and Technology (NIST) has developed several documents that may be considered "best practices" guidelines for industry and government cyber security programs. NIST makes these guidelines available through a number of ways, to include the issuance of its Special Publications (SP). Four such SP best practice guidelines are examined in this sub-section.

NIST SP 800-12: The NIST Handbook.

This Special Publication 800-12 (NIST 1996) is a comprehensive introduction to computer security, providing an overall look at how to establish an organization security program, to include a walk through of incident response procedures. SP 800-12 provides a general guideline for cyber damage assessment best practices and impact assessment. These are discussed in detail in subsequent publications.

NIST SP 800-61: Computer Security Incident Handling Guide.

This publication is intended to provide organizations with a best practices guide for cyber security incident handling and is especially geared towards newly formed incident response teams (Grance, Kent et Al. 2004). The document provides guidelines to assist the incident response team in performing technical damage assessment after the incident occurs. Additionally it provides guidance the impact assessment is an important, but distinctly separate assessment from technical damage assessment. The publication states that by "combining the criticality of the affected resources and the current and potential technical effect of the incident", a reasonable understanding of the impact may be gained (Grance, Kent et Al. 2004).

NIST SP 800-30: Risk Management Guide for IT Systems.

SP 800-30 is intended to enable an organization to accomplish its mission by understanding risk to improve the effectiveness of the organization's security program (Stoneburner, Goguen et Al. 2002). This document is noteworthy for several reasons, but especially since provides to organizations a best practices guideline to implement impact analysis. Impact analysis during risk assessment allows the organization to identify, understand, and document the potential impact if a system is lost or damaged due to a

cyber incident (Stoneburner, Goguen et Al. 2002, pp. 2-4). NIST SP 800-30 prescribes the documentation of several key attributes about the asset including:

- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity

This risk management framework provides explicit guidance for documenting asset vulnerabilities and impact analysis in the even the asset is damaged. It is important that organizations document this information prior to an incident to ensure that effective damage and impact assessment is possible after an incident occurs.

NIST SP 800-55 Security Metrics Guide for IT Systems.

This publication (Swanson, Bartol, et. Al 2003) is primarily intended to assist organizations develop metrics for their security program. There is little usable information in this document for development of damage assessment metrics. The assessment criteria are heavily focused on allowing the organization to assess its technological security controls intended to protect the organization's data

.

Section Summary.

This section examined two models that possess some degree of potential contribution to military application decision making. However, both models approach damage assessment from an economic standpoint. While either or both model may have some application to military decision making, the economic nature of the approach will limit both to only long-term, or strategic, use. Neither model is able to provide the

tactical or operational decision maker with situational awareness of how a cyber incident impacts the current mission in the appropriate time window, allowing the mission to conceivably be saved and loss of human life possibly prevented. The lack of such a model or methodology is underscored by the case study research into current damage assessment practices on Air Force networks. This research showed that current methodologies are non-standardized and producing non-validated damage assessment metrics. The usefulness of these methodologies for providing commanders with situational awareness of damage after an incident is highly suspect.

There are best practices for various aspects of computer security and incident response that have limited application to damage assessment efforts. These are published by the National Institute for Standards and Technology.

III. Methodology

Introduction

This chapter outlines the methodology for data collection and analysis. The subject matter involved with CDA-D/MIA research requires a qualitative approach. An interview methodology was employed to gather the data for analysis and resolution of the research questions.

Methodology and Research Strategy

Selecting the methodology best suited for a specific research effort is difficult, yet important decision. Quantitative research is the preferred method among researchers. This type of research is efficient and generally allows the researcher to identify causal relationships within the data (Leedy and Ormrod 2005, pp. 94). Quantitative research cannot easily capture complex phenomena such as human or organizational behavior, however (Stevens 2001).

Qualitative research, on the other hand, is well suited to "answer questions about the complex nature of phenomena, often with the purpose of describing and understanding the phenomena from the participants' point of view. (Leedy and Ormrod 2005, p. 94)" Strauss and Corbin (Strauss and Corbin 1990), provide five reasons for performing qualitative research:

1. The researcher's conviction based on research experience
2. The nature of the research problem
3. To understand a new or little understood problem
4. To gain new perspective on a previously well understood problem

5. To provide understanding of the details in complex phenomena that cannot be easily conveyed with quantitative methodology

Roberts notes that the qualitative approach to research is founded in the philosophical orientation called phenomenology, a discipline that focuses on first-person experience. Qualitative research strives to gain a holistic understanding of the studied problem. They collect data through methods such as observations, interviews, surveys, and even written documents. Qualitative research can focus on a range of complex issues ranging from the personal experience of individuals to organizational processes (Roberts 2004, p. 10). Qualitative research is an "umbrella term" that covers many different research strategies (Roberts 2004, p.11). Determining which research strategy to utilize can be difficult to accomplish. Yin (2002) provides a three-condition evaluation to assist in this decision:

- Consider the type of research question posed,
- Consider the extent of control the researcher maintains over the phenomena
- Consider the degree of focus on contemporary versus historical events (p. 5)

By applying these questions to a qualitative research strategy matrix, it is possible to determine a strategy best suited to the nature of the research (see Table 3 below). By testing the research questions posed in the introductory chapter of this paper against Yin's matrix, it becomes clear that no single research strategy perfectly fits the nature of the research questions. The questions explicitly ask *how* something can be done, with an implication that the research must discover both *how* it is being done now and why; what

historical events created the context in which damage assessment currently exists? This leaves three strategic possibilities:

- experiment,
- historical analysis,
- and case study.

Table 3. Relevant Situations for Research Strategies

Strategy	Form of Research Question	Requires Control of Behvioral Events	Focus on ContemporaryEvents?
Experiment	how, why?	Yes	Yes
Survey	who, what, where how many, how much?	No	Yes
Archival Analysis	who, what, where how many, how much?	No	Yes/No
History	how, why?	No	No
Case Study	how, why?	No	Yes

(Yin 2002, p. 5)

Since the research cannot control the events being studied, experiment is eliminated. Because the nature of this study fits both historical analysis and the case

study as suitable research strategy, this research elects to employ a hybrid strategy that employs elements of each.

This historical/case study hybrid study is warranted to ensure the investigative questions of this research are answered appropriately. It is commonly agreed in the network security community of interest that defensive cyber damage assessment methodologies are not as effective as they need to be. In order to answer the first investigative question, the research must examine how damage assessment is currently being done and identify where these shortcomings lie. The second and third investigative questions may be addressed in a similar manner, but each relies on the previous being answered. All of the investigative questions, however, make assumptions about mission impact assessment that must be addressed if the research is to be valid. For this reason, the research must understand the state of damage to mission impact mapping on Air Force networks and to identify what successes are present and what obstacles may be preventing efficient mission impact activities.

Instrumentation and Data Collection

This research attempts to answer its three research questions by first gaining an understanding of the effectiveness of damage and mission impact assessment on Air Force networks. This was accomplished through a combination of literature review, analysis of existing research, and interviews. It is common knowledge in the DoD that defensive damage and mission impact assessment is not being conducted as accurately and efficiently as it should be. However, the causes and possible solutions are widely debated. The data collected in this research provides a foundation for proposing a more

effective way to conduct cyber damage and mission impact assessment following a cyber security incident in a non-profit driven organization, such as the military.

Literature Review and Existing Research.

Yin states that existing documentation is a suitable data source in case study research (2002, p.86). Most of the documentation of damage assessment models and methodology is focused on organizations that operate for financial profits. Relatively little research has been accomplished in the area of damage and mission impact assessment in organizations not driven by financial profit; and therefore, some aspects of available literature and documentation did not directly fit. This is primarily true of the damage and impact models used by organizations that deal explicitly with various dimensions of financial loss caused by an incident. These are of little direct use by non-profit driven organizations. However, for-profit organizations struggle with the same problems as the latter in damage and mission impact assessment efforts. There was, therefore, a substantial amount of data available in the literature review that did applicable to this research effort that helped with identification of such problems in order to propose an improved methodology.

Existing case study research of damage assessment efforts on Air Force networks (Thiem 2005) provides further and more detailed insight to problems existing in damage assessment efforts specifically on Air Force networks. The existing research investigated cyber damage assessment methodologies used on Air Force networks by interviewing individuals intimately involved with both Net-D direct activities and Net-D command and control of incident response. When combined with the literature review data, a strong case may be built for determining the state of damage and mission impact

assessment on Air Force networks and visibility into some of the suspected causes. Understanding the causes coupled with additional literature documentation may enable development of new damage and mission impact assessment methodology.

Interviews.

The qualitative nature of the case study lends itself to the use of the interview as an investigatory instrument. The interview is one of the most important sources of case study information (Yin 2002, pp. 89-92). There are two general categories of interviews. The structured interview consists of the research asking a set of questions. This category is relatively rigid and leaves little room for the interviewee to discuss important related information that may lie just beyond the boundaries of the question. In such cases, important information may be missed. The semi-structured interview, also called an open-ended interview, the research can ask open ended questions or follow the standard question with a specific question tailored to the interviewee's experience to elicit further detail about the answer (Leedy and Ormrod 2005, p. 184; Yin 2002, p. 90).

Interview Structure.

The interview was specifically designed to address the second and third research questions. These questions deal specifically with the core issue of this research: mission impact assessment. The approach to the interview was to allow the professional experts in network defense incident response provide insight into the state of mission impact assessment. The interview was designed to allow each respondent to answer in his or her own way and provide details and perspective into the subject through individual experience. The intent was to elicit individual free formed responses providing multiple perspectives on the state of mission impact assessment as it is currently being

implemented on Air Force networks. Since successful mission impact assessment relies on multiple other areas to be performed effectively, responses to the interview questions would necessarily touch on the activities that enable mission impact assessment to function correctly. In this manner, the interview respondents will reveal the issues both contributing to and impeding mission impact assessment independently.

The interview was comprised of two distinct sections. The first section was simply to identify the interviewee's qualifications to provide valid responses to questions relating to the state of mission impact assessment on Air Force networks. The second section was comprised of three questions designed to allow the interviewee the opportunity to discuss the issues relating to mission impact assessment on Air Force networks.

Section 1 Questions.

This section is comprised of two questions to ensure that the interviewees have appropriate exposure to network defense and incident response activities to possess a reasonable observation of the state of damage and mission impact assessment on Air Force networks. The first question asked the following:

> *"Are you currently or have you recently (within the past 12 months) been professionally assigned to a position in Network Defense (Net-D) involved in incident response activities on Air Force networks, to include Network Operations command and control functions?"*

This question is designed to ensure that the interviewee has timely experience in a job with network defense incident response responsibilities.

The second question in this section was designed to allow the interviewee to list the type of involvement.

"In what capacity was this involvement? (For example, incident handling, forensic investigation, response command and control, etc.)"

Not all involvement possibilities were listed, allowing the interviewees to self-identify areas of incident responsibility that the researcher may have overlooked. The interviewees identified six distinct areas of responsibility in network defense incident response. These were:

- Initial incident response
- Incident handling
- Incident investigation
- Damage / Impact Assessment
- Incident Recovery
- Command and control

The demographics discussed previously show the areas of involvement of the respective interviewees. The range of involvement increases the likelihood of wider participant perspective of the issues affecting defensive cyber damage and impact assessment on Air Force networks.

Section 2 Questions.

This section consisted of three progressive questions to determine the state and effectiveness of mission effective. The first question was stated as follows:

1. "In your experience, does current incident damage assessment methodology on Air Force networks comply with the requirement of *CJCSM 6510.01 Ch 3 Annex A to Appendix B to Enclosure B* prescribing operational impact assessment of a DoD organization affected by a computer security incident?"

This question was to gain an understanding of the interviewee's perspective on whether Air Force damage assessment and mission impact efforts were meeting the requirements

(CJCSM6510.01 2006) for commanders to report how a network incident has impacted an organization's mission. The expected responses were a direct reflection of the interviewee's perception of these requirements as defined in the governing joint document.

The second question was designed to be a progressive path to allow the interviewee to discuss his/her perceptions about the Air Force's network defense incident response functions ability to meet this requirement. The question was stated as follows:

2. " In your experience, how well are responsible Net-D functions (incident response, forensics activities, etc.) able to estimate the impact to an organization's mission capability resulting from an incident on Air Force networks? "

This question was followed by the third question, which provided an opportunity for the interviewee to elaborate anything they felt was relevant to the previous question—but specifically those things that affected the damage and mission impact assessment actors to successfully and accurately accomplish these activities. The third question stated as follows:

3. *"Based on your response to question #2, what factors either contribute to or impede the ability to effectively estimate the impact to an organization's mission capability following an incident on Air Force networks?"*

Interview Conduction.

Interviews were conducted over the telephone. The respective organizations were contacted in advance and appointments made to formally conduct the interview. Each interviewee was asked all questions previously discussed. The interview was conducted in a semi-structured format to allow each respondent to discuss and elaborate on any part of the response he/she felt was relevant to the questions. The semi-structured interview

format allows the interviewee to discuss the context of his/her response to a particular question to reduce the likelihood of error introduced by misunderstanding by the interviewer of the context of the response.

Sample

The sample population was selected from Air Force active-duty members and civilians that are employed, or have been employed in the past 12 months, in a Defensive Network Warfare (Net-D) capacity. Interviewees in this sample must have experience with the incident response activities of Net-D provide usable data for this research. Specifically, the selected sample ranges from personnel with direct involvement in the technical aspects of network defense incident response to command, control, and coordination of Net-D activities at a level appropriate to understand "the big picture" of how damage and mission impact assessment support the operational mission at both the organization and enterprise levels. By necessity, this requires that participants work in the top "tier" of network defense operations. These operations are, in fact, divided into three operational tiers (see Figure 7 below). Network operations command and control of incident response and the incident response experts reside at Tier 1 and work with the responsible agencies at the subordinate tiers to ensure effective incident assessment, response, handling, investigation, and remediation. Agencies at Tier 1 interact with all levels and directly plug in to the Joint GIG, providing it personnel with a unique perspective personnel at subordinate levels may not possess. For this reason, the interview targets personnel employed in network defense incident response activities at Tier 1.

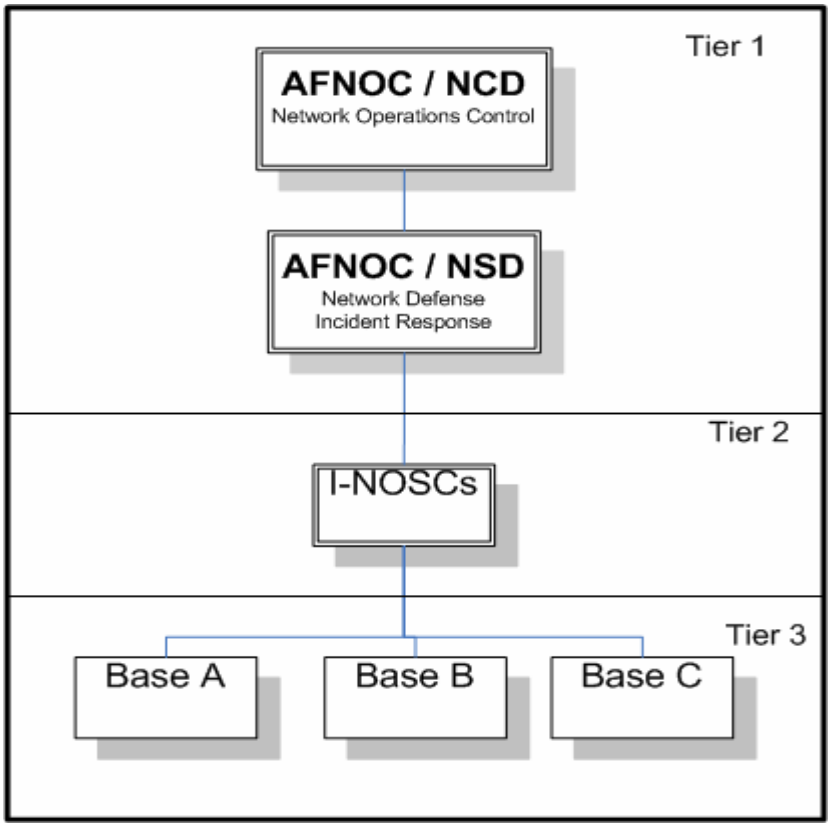


Figure 7. Network Defense Tiers of Operations

It must be noted that this produced a situation where the views of the interview responders are relatively homogenous in their experience and perspectives. However, this issue is a necessity to ensure that all respondents possess the appropriate professional and personal experience to make qualified and reasonable independent judgments regarding the state and effectiveness of mission impact assessment as it is currently being implemented. Allowing personnel with little or no experience in cyber damage and mission impact assessment on Air Force networks would certainly introduce weakness in the data collected in the interviews.

Interviewees were self-selected by volunteering to participate in the research data collection. No personally identifiable information was collected on the interviewees.

Data Analysis Procedures

There are various approaches to qualitative data analysis, with some being more suited to certain situations than others (Lacity and Janson 1994, pp. 138-140). Lacity cites three general approaches to text analysis with each being dependent on assumptions, to include the role of the researcher (see Table 4 below). Because damage mission impact assessment activities are dependent on such a wide range of supporting activities, it is important that the researcher have an understanding of the network defense incident response and damage assessment environment to be able to accurately understand and interpret the qualitative data collected. In this sense, the researcher must be an insider, to some degree, to understand the wide range of issues that may be discovered during research. For this reason, Lacity suggests that an interpretive approach to qualitative data analysis be used (1994, p.140).

Table 4. Lacity Text Analysis Framework

Assumptions					
Text analysis approaches	Research method	Nature of text	Role of researcher	Validity checks	Examples
Positivist	Identification of nonrandom variation	Objective	Outsider	Quantitative	Content anlaysis Verbal protocol analysis Script analyisis
Linguistic	Study language relationship	Emergent	Outsider	Primarily Qualitative	Speech act analysis Discourse analysis
Interpretivist	Analyze the cultural	Subjective	Insider	Qualitative	Hermenutics Intentional analysis

(Lacity and Janson 1994, p. 140)

Intentional analysis is form of interpretivist data analysis that attempts to understand the speaker's intention. It assumes the research and interview have similar background in the research subject allowing the research to better understand the contextual factors that influence the research subject (Lacity and Janson 1994, p. 151). Intentional analysis allows the researcher to discuss with the participants the meaning they ascribe to their experiences. Lacity states that this method is particularly appropriate for analyzing data collected in interviews and consists of four steps of analysis; described as follows:

> *"In the first step of the intentional analysis, the researcher describes the* 'facts' *of the phenomenon.* 'Facts' *are socially shared realities agreed upon by all participants. For example, the analyst and payroll clerk may both attest to the "fact" that two payroll programs need to be changed.*

> *In step two, the researcher determines the way participants ascribe meaning to their separate realities by how they perceive cause and effect. For example, the analyst may claim, "I decided to fix the payroll calculation first because if it were not fixed this week, people's paychecks would be wrong next week." Here the systems analyst perceives her behavior in terms of cause (erroneous payroll calculation program) and effect (erroneous payroll checks).*
>
> *In step three, the researcher identifies themes- or invariants -- that emerge from the text. The researcher then identifies themes that are used to develop common interpretations for an entire class of phenomena. For example, assume the researcher studies the entire set of relationships between information systems personnel and payroll personnel. A potential theme may be that systems personnel consistently prioritize users' requests.*
>
> *In step four, the researcher abstracts the "essences" from the text. Essences are wholly subjective gestalts what is learned from studying the phenomenon. Abstracting essences requires creativity, intuition and reflection. The researcher no longer asks "What do the participants think about the phenomenon?" but rather, "What do I think?"* (1994, p. 151)"

After the interview data was collected the responses for the three investigative questions of the interview are coded to allow graphical 'mapping' of the response data.

Limitations

This research effort maintains several limitations. The sample size is small. Ideally, a study attempts to obtain interview data from a large pool of potential interviewees to develop a more accurate picture of the problem. This is especially true for the intentional analysis method employed in this research. A larger sample size would better demonstrate agreement in the both the *facts* (Lacity 1994, p. 151) and the contextual influences reported by the interviewees. However, it was important that personnel providing the data posses adequate experience and skill set to make qualified

and valid responses to the interview questions. This, by necessity, reduced the sample size.

Another limitation is the introduced by the nature of intentional analysis. The very quality that lends intentional analysis to interview data analysis, the common contextual factors between the subjects and researcher, introduces some degree of bias. It must be noted that the researcher was previously professionally engaged in network defense incident response activities on both Air Force and joint networks. The experiences gained were among the motivating factors for this research effort. Qualitative research inevitably introduces some degree of reflexivity (Leedy and Ormrod 2005, p. 285), but all efforts to maintain objectivity and minimize bias introduced by this phenomenon.

The scope of this paper is also a concern. In most research, the scope is brought down to a near level to allow the researcher to get close to the research subject in great detail. Indeed, this was the initial goal of this research effort. However, as research progressed through the methodology described above, it became apparent that the lack of research in this area created as situation where the current damage assessment and mission impact assessment methodology as a whole must be examined to accurately and effectively address the investigative research questions. This fact prevented any one part of the current methodology to be examined in great detail without overlooking serious factors that contribute to the problem being studied. As a result, the research scope is at the lowest level to provide a look at a comprehensive methodology, in hopes of producing satisfactory and effective recommendations for an improved methodology, which is the ultimate goal of this research effort.

Chapter Summary

This research attempts to answer three questions for which there is no quantitative data available. The qualitative nature of the subject lends itself to a historical analysis/case study hybrid research strategy. An examination of existing research provides some of the research context, but for a better understanding of the defensive cyber damage and mission impact assessment climate on Air Force networks, it is important to conduct interviews with the personnel actively engaged in these activities. Understanding why damage and mission impact assessment is not effective is extremely important to answering the investigative questions of this research.

IV. Results and Analysis

Introduction and Overview

It is well known and commonly agreed that defensive damage and mission impact assessment cyber security incidents on Air Force networks is not being performed as effective or efficient as it needs to be. This research has collected data through extensive literature review, case study research on damage assessment on Air Force networks, and interviews with personnel directly professionally involved with network defense incident response activities. This section will analyze and discuss the results of the collected research data; and is the most important part of the research effort. Here the collected data will be presented and interpreted so that intrinsic meanings may be revealed to build a whole picture of the problems, ultimately leading to answers to the investigative research questions posed in the opening chapter.

Chapter Structure.

The data analysis of this chapter will present and discuss the interview data first. Although the interview questions specifically address the second and third investigative research questions, the semi-structured format allowed the interviewees to provide additional data that they felt was relevant to the specific questions. Some data in the interview responses has relevance to the first research investigative question regarding cyber damage assessment.

Next, the chapter will discuss the findings about the state of cyber defense and damage assessment currently employed on Air Force networks. This analysis is based on literature review data and existing case study research (Thiem 2005). The final part of

this chapter will provide a synthesis of collected data and discuss the findings to each of three investigative questions of this research.

Approach to Analysis of Research Questions.

The purpose of this research is to determine an effective and accurate methodology for defensive cyber damage assessment on Air Force and DoD networks. Three investigative research questions were formulated to build the framework for this research effort. These questions are:

> *R1. How can the damage resulting from a successful cyber attack be effectively measured in a non-profit driven organization?*
>
> *R2. How can such damage be mapped to impact to an organization's mission capability?*
>
> *R3. How must this assessment be reported to the decision maker to maximize the quality of the assessment for use as decision input?*

To answer these questions correctly they must be approached and answered in order. The research must first establish how damage is currently being assessed before proposing how damage assessment may be effectively measured in a non-profit driven organization. As previously stated, it is common knowledge that there is ample room for improvement in the assessment of cyber damage and mission impact arena; so analysis will begin by laying out the facts provided by the data and identifies areas needing improvement as they relate to the research questions.

Interview Data Analysis

Intentional analysis was applied to the transcripts of the interviews. Lacity states that intentional analysis is a form of interpretivist analysis that is well suited to this

particular research effort since the researcher may discuss the contextual meaning ascribed to experiences relayed in the interview. This provides a more richly descriptive response to the questions posed during the interview (Lacity 1994, p.151).

Intentional analysis is a four-phase process. The first three analyze the facts, contextual perceptions issues of the respondents, and common themes presented by the interviewees. In the fourth phase, the research abstracts the *essences* of the text, as a whole (Lacity 1994, p.151).

The first section of the interview establishes respondent qualifications to establish respondent demographics. Intentional analysis will not be used on the questions in the section, and this data is discussed in the following the following section of this paper. Intentional analysis is applied to the data collected in the second section of the interview.

Interview Sample Demographics.

It was previously noted that the interview sample size was small. The nature of the research required that the pool of potential interviewees be small by necessity. The purpose of the interview was to understand the effectiveness of mission impact assessment as it is currently being implemented on Air Force networks. It is important to identify any obstacles or catalysts to these efforts. For this reason it was essential to limit the potential sample population to only those respondents possessing relevant experience in network defense incident response activities. To ensure accurate responses were formed both from relevant experience and appropriate perspective in this area, the potential interviewees were purposefully limited to current or recent employment in a job with direct network defense incident response responsibilities at the Tier 1 level of network defense incident response activities. These agencies at the Tier level are the

agencies tasked by the Air Force to lead and execute efforts for incident response, damage assessment and containment, mission impact assessment, and remediation and recovery following an incident on Air Force networks; and ensure netops integration with DoD networks. The pool of potential interviewees was intentionally inclusive of those performing direct technical response, as well as those responsible for the command and control of NETOPS activities as they pertained to Net-D incident response coordination and actions. This was important to the research as it ensured a full range of perspective into the capabilities and limitations of current mission impact assessment efforts.

There were approximately 18-20 personnel identified as potentially qualified interviewees. Participation was voluntary and participates were advised that no personally identifying information would be collected which could attribute any responses to them. Not all potential interview candidates elected to participate, however. Due to the voluntary nature of the sample selection, data on the reasons for participation declination was not collected. Leedy and Ormrod note that this is a common occurrence (Leedy and Ormrod 2005, pp. 184-185).

In all, nine personnel agreed to be interviewed. All nine acknowledged that they were currently or and recently been assigned to a position in which their primary duties involved responsibilities directly related to network defense incident response and response support activities shown in the following table (see Table 5 below). This table breaks the roles of network defense incident response involvement into six categories:

- Initial Incident Response: Those activities associated with confirmation and declaration of an incident and the coordination of initial response activities from Tier 1 to Tier 3.

- Incident Handling: Those activities associated with the documentation, tracking, and administrative issues of network defense incident response.

- Incident Investigation: Those activities directly associated with investigating how the incident occurred and what systems were affected.

- Damage/Impact Assessment: The assessment and reporting of technical damage and/or mission impact assessment.

- Incident Recovery: Those activities associated with returning the effected systems to service, while simultaneously supporting ongoing incident response activities.

- Command and Control: Those activities associated with the coordinating and directive actions of incident response as they relate to netops activities.

Table 5. Interviewee Involvement in Network Defense Incident Responsibilities

Interviewee Number	Initial Incident Response	Incident Handling	Incident Investigation	Damage / Impact Assessment	Incident Recovery	Command Control
001	x	x	x	x	x	x
002	x	x	x	x	x	x
003	x	x	x	x		
004	x	x	x	x	x	
005			x	x	x	
006	x			x		x
007	x			x	x	x
008	x	x	x	x	x	
009	x			x	x	x
Totals:	*8*	*5*	*6*	*9*	*7*	*5*

Of these nine, eight were responsible for initial incident response activities. Five reported that they were currently or had been directly involved in incident handling efforts. Six indicated experience in incident investigation efforts. Seven had been involved with incident recovery efforts after an incident. Five were responsible in some way for command and control of incident response activities. All responded that they were involved in some aspect of damage and mission impact assessment efforts.

All interviewees were currently or had recently been responsible for multiple aspects of incident response activities. Two interviewees were currently or had recently been involved in all aspects of the incident response process. Only one respondent was neither involved in initial incident response nor command and control activities. This interviewee likely specialized in technical aspects of incident investigation and recovery.

Intentional Analysis of Interview Response Data.

This section discusses the interview response data. Lacity defines the data *facts* as the "shared realities agreed upon by all the participants (1994, p.151)." Since the pool of individual interviewees may hold differing perspectives on the same problem, this section will discuss the data in terms of commonly shared facts, conflicting data, and any unexpected findings in each question.

Fact Analysis of Section 2, Question 1.

The first interview question of Section 2 was:

> "In your experience, does current incident damage assessment methodology on Air Force networks comply with the requirement of *CJCSM 6510.01 Ch 3 Annex A to Appendix B to Enclosure B* prescribing operational impact assessment of a DoD organization affected by a computer security incident?"

This question elicited a unanimous negative response. All nine interviewees cited that the current incident damage assessment methodology on Air Force networks is not meeting the intent of this requirement for mission impact damage assessment reporting. All but one respondent elaborated on this question in some way by stated that mission impact assessment is being attempted, but is not being carried out effectively. Three respondents stated in this question that there are breakdowns occurring at the Tier 2 and

Tier 3 levels that prevent effective mission impact assessment. The others deferred to question 3 to provide additional information.

The nature of these responses were expected since it is commonly accepted the current damage and mission impact assessment is not being performed at an effective level. There were no unexpected responses to this question.

Fact Analysis of Section 2, Question 2

The second question of this section was:

> "In your experience, how well are responsible Net-D functions (incident response, forensics activities, etc.) able to estimate the impact to an organization's mission capability resulting from an incident on Air Force networks?"

This question gave the interview respondents the opportunity to provide independent evaluation of how each viewed the effectiveness of the Air Force's implementation of mission impact assessment. The responses to this revealed general agreement that the current implementation of damage and mission impact assessment is not doing an effective job. A general agreement was expected for the same reasons stated in the analysis of Question 1.

Since the response to this question was free-formed, all interviewees respond with *soft* responses to this question, meaning that that no respondents provided a direct answer, such as "*we're doing a poor job."* Possibly, due to the wording of the question, all respondents provided answers that were more suited to a performance range, rather than a discrete performance value. Examples of answers to this question ranged from, "*somewhere between a bad job and a really bad job*" to "*we're doing the right things in some areas, so overall we're doing alright but still need to improve a lot*." This type

qualitative response is difficult to measure, so to capture the intent of these responses, the responses were coded as ranges of performance. The coding was based on a five-point graduated scale from very poor to excellent. Each point on the scale was assigned a coding value as follows: very poor = 1, poor = 2, moderate = 3, good = 4, and excellent = 5. The coding for each question was assigned to reflect the overall nature of the response to this question. Each respondent's answer was coded as a *range* of two values that best reflected the respondent's response intention and the range was averaged to produce a score, as shown in the raw data table for this question (see Table 6 below). This coding was designed only to aid in understanding the trends among the qualitative responses to this particular question through a visual representation of the responses.

Table 6. Coded Response Ranges for Interview Section 2, Question 2

Interviewee Number	Very Poor	Poor	Moderate	Good	Excellent	Scores
001		2	3			2.5
002	1	2				1.5
003	1	2				1.5
004	1	2				1.5
005	1	2				1.5
006	1	2				1.5
007		2	3			2.5
008		2	3			2.5
009			3	4		3.5
Totals:	*5*	*8*	*4*	*1*	*0*	
Rating Value:	***1***	***2***	***3***	***4***	***5***	

The attitudes of nearly all interviewees' responses to this question tended towards the lower end of the coding scale. Five of the nine respondents provided a response that indicated the Air Force's implementation was *poor to very poor*. Three provided

responses indicating that the Air Force's ability to estimate mission impact after a cyber incident is only *poor to moderate.* One respondent stated that "we're not there yet, but we are getting better that we were." This respondent still did not give high marks to the current process, but indicated perceived performance in the *moderate to good* range.

Expected Results.

The researcher expected a wide range of responses with the respondents closer to the "operational end" judging mission assessment efforts to be less effective than those handling the more technical issues involved with damage and mission impact assessment. This expectation was based on the researcher's experience and analysis of existing literature and research that indicated the strong focus on technology that exists in Air Force Net-D activities.

Question 2 Findings.

The data collected for this question produced the opposite result as those expected by the researcher. The data showed that the majority of those involved in operational command and control positions held a relatively more favorable view of mission impact effectiveness than did those involved with the technical aspects of damage and mission impact assessment. This finding is very important to this research, especially when considered in context with the data in Question 3. It is also important to note that only one respondent rated damage assessment as moderate to good. The majority of responses evaluated the effectiveness of mission impact assessment efforts as poor.

Fact Analysis of Section 2, Question 3.

Question 3 was stated as follows:

> "Based on your response to question #2, what factors either contribute to or impede the ability to effectively estimate the impact to an organization's mission capability following an incident on Air Force networks?"

This final question provided the interviewees the opportunity to elaborate on the issues that they viewed as affecting their assessment of question 2. The question produced several common but independently provided responses that the interviewees felt were at the core of the problems with cyber damage and mission impact assessment. The first and most common was that the wrong agencies are being tasked to perform mission impact assessment. Seven out of the nine interviewees made direct reference mission impact assessment being the responsibility of the system or asset owner; but that the responsibility is resting with the incident response agency to determine the damage and impact to the organization's mission. Three of the respondents stated that this reliance on the wrong entity existed in all three operational tiers, but was most problematic in the Tier 2 and Tier 3 levels. When an incident occurs, commanders at base and Tier 2 levels expect the technical experts of the 33 IOS to tell the commander how his/her mission was affected. All three respondents assert that this is a task that cannot be accomplished by an agency external to the organization whose mission was affected by the incident. These respondents state that the organization that owns the mission must bear the responsibility for mission impact assessment since only it can possess visibility of the relationship between the systems, the information, and the mission.

A second common problem cited by six of the nine respondents is the local commanders rely upon base-level system administrators that are improperly equipped for damage assessment responsibilities. Five of the respondents cited this as a training and

education issue. Four respondents reported that the Tier 3 administrators tasked to work with Tier 1 responders to perform local damage and mission impact assessment regularly provide incorrect or meaningless damage and mission impact assessment information. Two respondents noted that there have been many cases where Tier 3 administrators provided fabricated damage and mission impact assessment information because the did not understand the relationship between the system and the mission. Several respondents stated that these system administrators lack essential technical skills to perform the mission impact, even with the assistance of the incident response agent, which compounds the problems of determining damage and mission impact.

It is also important to note that two respondents explained the problem being that the incident responders work with system administrators belonging to the organization affected by the incident, not than the system users. These system administrators are neither users of the affected system, nor have an understanding of how the information processed by the system supports the organization's mission. The information reported back to the incident responders is strictly limited to technical information that has no factual mission impact relevance. One interviewee cited that the system administrator intentionally provided impact reporting metrics from a system unaffected by the incident because it was easier than getting it from the affected system. This, of course, negated any benefits of damage and mission impact efforts; and the interviewee attributes the problem as a lack of understanding of the damage assessment process that is a direct result of a training failure.

Another important issue mentioned by several of the respondents was a perceived misunderstanding of the role of technical assessments performed by the network defense

incident response agents. The interviewees that mentioned this as a problem stated that often commanders misunderstood the role of the technical assessment as a substitute for the mission impact assessment. These respondents stated that this failure to understand the role of the technical assessment as a foundation for mission impact caused problems and "push back" from these units at both a system administrator and command level. The interviewees stated that this friction slowed and occasionally crippled mission impact assessment efforts after an incident.

An associated issue mentioned by several of the respondents was a perceived misunderstanding of the role of the technical assessments performed by the network defense incident response agents. The interviewees that mentioned this as a problem stated that often commanders misunderstood the role of the technical assessment as a substitute for the mission impact assessment. These respondents stated that this failure to understand the role of the technical assessment as a foundation for mission impact caused problems and "push back" from these units at both a system administrator and command level. The interviewees stated that this friction slowed and occasionally crippled mission impact assessment efforts after an incident.

A third common issue was that a lack of understanding of the relationship between the system and the information used by the system to support the mission exists. This is similar to the previous issue, but differs in perspective. The previous facts identified the misunderstanding as a result of technical training failures. Five of the nine respondents to this question independently provided anecdotal examples of breakdowns in cyber damage and mission impact efforts directly attributable to a focus on the system technology such that the connection to the mission not understood. All five who cited

this as serious problem included examples of the focus on the technology and a failure to understand that the system processes information supporting some aspect of mission operations. Two respondents specifically relayed that this misunderstanding exists in both the command structure and the technologically focused system administrators on which the commander depends. One respondent stated, "Its common sense, but the commanders don't get it and the system admins don't get it. It's a simple concept, but they're missing that the data and information processed on the system is what is important to the mission." Another interviewee referring to this same problem responded that, "the Air Force is sometimes blinded by technology…which leads to a misunderstanding of what can and can't impact the mission." Four of the respondents relayed problems that this lack of understanding made it impossible to determine second order impact elsewhere in the Air Force enterprise.

Another response commonality supported the previously discussed issue. Three respondents stated that the problem of failing to understand the system to mission relationship was compounded by a lack of usable documentation listing the assets owned by the organization and the associated relationship to the mission. These respondents independently noted that the documentation that did exist, such as system accreditation packages, was not conducive to cyber damage activities since it primarily focused on technical issues. One respondent noted that the system administrators, not being users, could not use this documentation to understand how to the affected system supported the organization's mission. Two respondents stated that mission impact assessment efforts could be enhanced if documentation of the systems contents and support for the

organization's mission was documented at some time prior to the occurrence of an incident.

Expected Results.

The researcher expected a wide range of "problems" to emerge from the data collected from this interview question with the hope the several central themes would emerge. The hope is that the emergence of these themes would create a "path" to lead the researcher to the source of the problems. These themes did in fact emerge. The majority were in the general area expected by the researcher, but there were some surprises that uncovered unexpected problems in the mission impact assessment processes that the researcher had not previously considered.

Question 3 Findings.

The fact analysis has identified commonly agreed upon "facts" reported by the nine respondents. However, there were also interviewees that felt a strong focus on technology was important and appropriate. One interviewee stated that the technical assessments produced by the incident response agents was meeting the needs of cyber damage assessment, and the problems with mission impact assessment lay with incompetence at the "NOSC and base-levels". Additionally, although all interviewees agreed that mission impact assessment is falling short of its mandate, not all agreed on the cause of these shortcomings. The consistencies in responses have been discussed, but there also areas of non-agreement that were mentioned by individuals. For example, one respondent felt that the DoD netops function was asserting too much authority into the implementation of network defense and mission impact efforts on Air Force networks. This respondent felt that this was creating unnecessary work and constraints on the

incident response efforts. Another respondent independently provided a countering view to this by stating that the current efforts in mission impact assessment were not providing sufficient upward feed to the commanders watching the overall health of the GIG and the mission operations that are supported by the GIG. This respondent established that Air Force networks are only one piece of the GIG, and mission impact assessment activities on Air Force networks must provide sufficient support to the higher-level missions. This respondent also noted that *the big picture* is often forgotten by those focused on technical issues.

Another difference worth noting was that two of the respondents expressed a feeling that those involved in the command and control aspects of incident response activities did not possess an understanding of the problems that were preventing successful mission impact assessment. One respondent with command and control experience responded that those agents responsible for technical mission impact assessment activities, were not providing mission impact assessment reports in a timely fashion. As a result, mission impact reporting negatively affected since commanders could not get results quickly.

Intentional Analysis of Contextual Perceptions in Responses.

The demographics of the sample population were discussed previously in this chapter. It worth stating again, however, that the sample of interviewees was small and relatively homogenous by necessity. Since interviewees were self-identified, it became important that the pool of potential interview respondents be comprised of individuals with appropriate professional experience in cyber damage and mission impact assessment on Air Force networks to provide accurate and qualified individual responses to the

interview questions. All interviewees must possess current or relatively recent professional experience in network defense incident response activities. As a result the interview respondents possess similar contextual perceptions about cyber damage and mission impact assessments on Air Force networks. This may be considered an explanation for the great consistencies in the *facts* reported by the interview respondents. However, the fact that all respondents agreed that mission impact assessment efforts are failing to meet the intent of joint guidance points towards the thematic problem area in current efforts. This is important because it must also be remembered that the interviewees work in differing areas of network defense incident response, providing each with a potentially unique perspective on the problems and strengths of these activities. Yet, these contextual differences allow interviewees to arrive at similar conclusions about the problems. The differences in responses are few and are mainly attributable to personal perceptions of responsibilities between the agents providing coordination and oversight and those performing technical assessment.

Intentional Analysis of Findings in Interview Responses.

There is general agreement that the current implementation of damage and mission impact assessment on Air Force networks is not being conducted effectively. As can be seen in the following chart (see Figure 8 below), the majority of respondents with command and control experience rated the effectiveness of mission impact assessment as between moderate and poor. This was a higher assessment than provided by those with more technical involvement. All but one respondent without command and control experience rated current damage and mission impact assessment between very poor and poor.

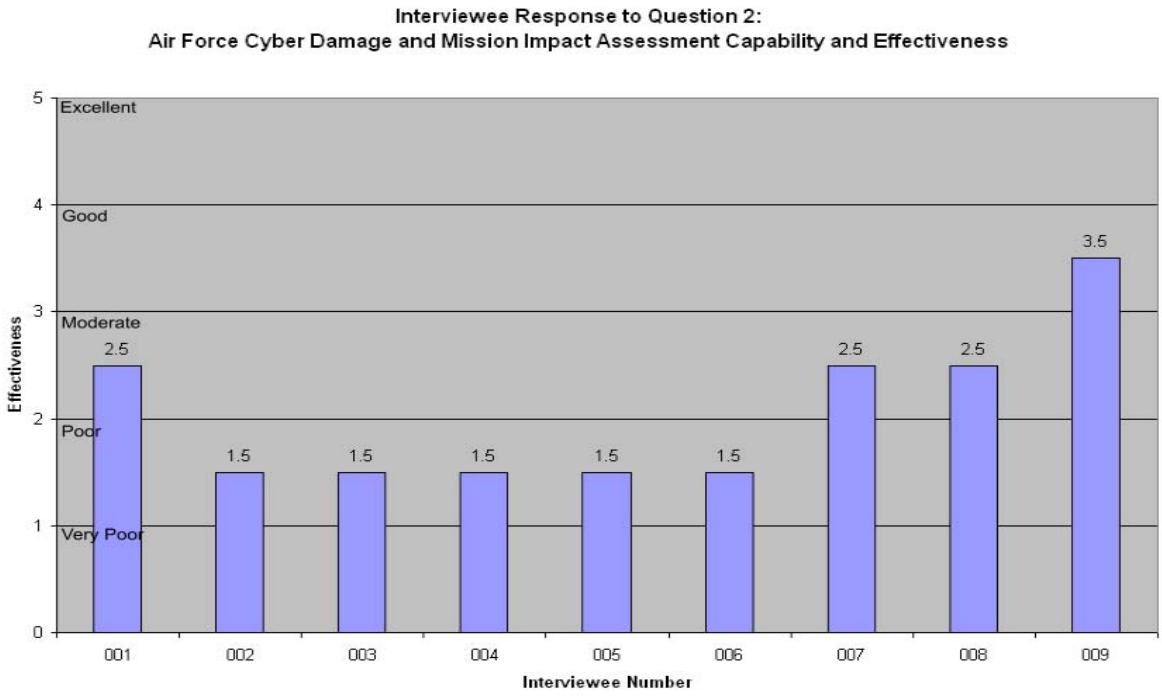


Figure 8. Bar Chart Results of Interviewee Response to Section 2, Question 2

Question 3 allowed respondents to independently identify issues that the respondent felt impeded or contributed to effective mission impact assessment efforts. There were several themes that became evident when all interview responses were examined. These can be summed up in the following bullets:

- Mission impact assessment and reporting must be accomplished locally
- Organizational Failure to Understand System to mission relationship
- Current mission impact assessment is too heavily focused on technology
- Current mission impact assessment is not producing usable metrics
- New perspectives introduced by mission impact assessment

These themes will be discussed in the following subsections.

Mission Impact Assessment Must Be Accomplished Locally.

Data collected in the interview process revealed that the current implantation relies heavily upon the incident responders to assess both the damage caused by the incident and the associated mission impact related to this damage. The current state of mission impact assessment is evidence that this approach is not working. The Air Force is an enormous enterprise with each organization having a specialized and independent mission that provides direct support to one or more additional missions in the enterprise. Cyber security incidents that occur on Air Force and DoD enterprise networks require that an incident response agent that is external to the affected organization come in and provide a technical assessment of the damage incurred by the incident. In nearly all cases, the response agent is entirely unfamiliar with the affected organization's mission. Mission impact requires that the assessor have an understanding the affected assets' relationship to the organization's mission. Such a task is impossible for an external agent to perform, as the interview respondents have noted. As a result, the mission impact assessments are best guesses based on an extremely limited understanding of the organization's mission. Accurate damage assessment is dependent upon mapping damage to the organization's asset to it mission in order for mission impact to be understood. The majority of respondents identified this problem as one of the chief impediments to effective damage assessment on Air Force networks.

Organizational Failure to Understand Mission Relationship.

The second theme presents a problem for local mission impact assessment. The ability for an organization to be the primary agent in local mission impact assessment

assumes that the organization understands how its systems support its mission. The failure of Air Force organizations to understand this relationship is a pervasive theme throughout the interview responses; and a serious obstacle to effective mission impact assessment efforts. The respondents cite that this failure to understand the critical mission support relationship exists in all levels of the organization, but especially in the command structure. Most commanders view a cyber security incident on the networks as a technical issue and rely exclusively upon their system administrators to provide local input for damage and mission impact assessment. There are many problems that result from this approach, the chief problem being that the system administrator is not a system user. The system administrator has a technical responsibility as the organization's cyber infrastructure custodian. The system administrator simply does not possess the perspective in to the use of the system, and rarely possess an understanding of how the system supports the organization's mission.

Interview respondents alluded to this problem multiple times in different ways. The common issue was centered on the problem that neither commanders nor the system administrator understood how the information the system processed was used within the mission. This is evidence that there is no understanding of information ownership within the organization; and no concept and assignment of information ownership within the organization. The commander is tasking the information custodian to perform an assessment that only the information owner would have the perspective to perform. It is particularly important to note that several of the interviewees made this point by specifically citing this failure of the organizations to understand that the systems process information supporting the mission. This underscores the kernel of understanding that

information is the asset within the organization. By failing to understand this ownership is not established. By failing to establish ownership of the information, mission impact assessment is unfocused and unproductive. Commanders must have a mechanism by which to establish information ownership, thereby allowing mapping of information assets on the affected systems to the mission which they support. Additionally, commanders must realize that the system administrator is the information custodian, not the information asset owner. The system administrator may not be equipped to perform accurate damage assessment without the necessary technical skills and understanding of the value of the information on the affected system

Heavily Focused on Technology.

There is agreement among the interview respondents that mission impact assessment is not being conducted effectively. Causality is extremely difficult, if not impossible to establish without "hard" data. However, based on the responses provided by the interview subjects and themes discovered in existing research on cyber damage assessment on Air Force networks the researcher asserts that the Air Force maintains too strong a focus on technology that is obstructing its ability to conduct defensive cyber damage and mission impact assessment accurately and in a timely manner.

The Air Force has always considered technology to be an important mission enabler. However, the interview responses indicate that too heavy of a focus on technology may be impeding mission impact assessment efforts. This issue is a consistent theme in a majority of the interviewees' responses and must not be downplayed. Six of the nine respondents directly attribute this issue as a contributor to the problems with current mission impact assessment efforts. The respondents report that

this problem manifests itself in many ways. The responses indicate that this focus on technology has created confusion about cyber damage determination and mission impact assessment methodology that is prevalent throughout the Air Force structure. Commanders view mission impact as a technical issue. They then find that the technical and economic metrics produced by the current cyber damage and mission impact assessment methodology are not applicable for decision making input for their mission operations. The results of the interviews indicates that the technologically focused approach is not working well for Air Force mission impact assessment and a new approach that facilitated mission impact assessment.

The problem with technological focus manifests itself in many ways, and the symptoms may be mistaken for the illness. This researcher asserts that the problem lays in the identification of technology as assets, rather than the treating and viewing the information the system processes as an asset. This view is supported by many of the respondents that indicate the focus on system technology is causing confusion and misunderstanding about the role the system plays in supporting mission objectives. This is tied to the concept of value; a term not specifically used by any of the respondents, but the concept was prevalent by those respondents that discussed the relationship between technical cyber damage assessment and mission operations impact assessment. These respondents used terms such as “worth” and “important to the mission” when discussing the data and information processed on the systems affected by the incident. The implications are that this information has value to the organization. It follows, therefore, that one of the key failings of technical focus to establish value meaningful to mission impact assessment and mission operations decision-making.

Lack of Asset Documentation.

Many of the respondents noted that organizations did not understand the relationship between the systems that they used and the mission operations the systems somehow supported. Several of the respondents noted that no usable documentation exists to facilitate this understanding. Documentation such as system accreditation packages exists, but are by design technologically focused and are not providing the local system administrator the perspective needed to perform mission impact assessment. The respondent indicated that mission impact assessment efforts would benefit greatly from documentation accessible to both the local system administrator and the incident response agency that would facilitate a better understanding of the system value and utility to the mission, but understanding the value and utility of the information stored on, or processed by the system as it supports the organization's mission operations.

Failure to producing usable and meaningful metrics.

Based on the interview responses and the interview data, the researcher asserts that the technical focus is resulting in an unusable mission impact assessment product. This is not a surprising finding since it was reported in several of the responses. The focus on technology leads to the exclusion of other important issues in mission impact assessment, and indeed, risk management and cyber security on the whole. Since the current cyber damage and mission impact assessment methodology exclusively relies on technologically focused methodology and agents to accomplish mission impact assessment, the result is a technologically focused product that cannot comprehensively measure mission impact accurately and provides unusable and applicable reporting metrics to the organization's commander.

This is true because the value presented by information technology is limited in scope, and attempts to determine damage to technology traditionally produce economic-based metrics; and these metrics are not helpful to standard military operations. This is a failure to produce usable metrics. Attempts to measure mission impact through exclusively technical metrics cannot capture all the potential mission impact which may result from a cyber security incident. This is a failure to produce accurate metrics. Currently commanders are gaining neither usable nor accurate measurements as a direct result of the problems identified in the interview process.

State of Defensive Cyber Damage Assessment on U.S. Air Force Networks

This section discusses the findings of an extensive examination of literature review, existing related research, and interviews of personnel with professional first-hand knowledge of the state of network defense activities on Air Force networks as they relate to defensive cyber damage and mission capability impact assessment. It is commonly agreed that the current methods of cyber damage assessment and mission impact assessment need to be conducted with more accuracy and effectiveness. Research of cyber damage assessment methodologies have shown that such efforts are being employed ad-hoc and with neither standardization nor validation (Thiem 2005, p. 43). Furthermore, the models they rely upon are producing ineffective and irrelevant assessment report information since they measure damage exclusively in terms of recovery costs and infrastructure availability. These metrics provide insufficient information to the commander to present an accurate picture of impact to the organization's mission operations.

Air Force guidance (AFI 33-138 2004) has designated the Air Force Network Operations Center (AFNOC) Network Security Division (NSD) as the agency responsible for leading incident response efforts on Air Force networks. The AFNOC/NSD is tasked to lead and coordinate damage and impact assessment of an organization's mission capability following a successful compromise. This is an extremely difficult and often impossible task under the current implementation of security management practices on Air Force networks.

In this section, the findings of literature review, existing research, and interview response data are examined to paint a clear picture of the factors that are confounding efforts to perform accurate and timely defensive cyber damage assessment and mission capability impact assessment. By understanding and documenting these factors the stage is set for answering the investigative questions of this research.

Current Approach to Cyber Security.

The Air Force's Network Defense (Net-D) activities are exclusively focused on the network technology rather than on the information assets contained within the information systems. Net-D is highly effective at defending networks. However, a technologically focused network defense scheme cannot work alone and Net-D must be part of a larger information protection scheme. The areas of responsibility assigned to the Net-D function are blurred. In practice, the Air Force tends to rely exclusively on the Net-D function as the vehicle for all aspects of defensive cyber operations; to include cyber damage and mission impact assessment. Literature review, existing research (Thiem 2005) and interview data demonstrate, however, the damage and mission impact assessment efforts are falling down in terms of providing effective and useful metrics.

Net-D is the implementation of technological security policy to establish technologically secure networks. The technologically exclusive approach of Net-D acknowledges the existence of data within the infrastructure, but cannot value it as an asset. Without explicitly recognizing and acknowledging information as an asset that directly supports mission operations, one of the chief failings of a highly technologically focused approach to cyber security is exposed in terms of damage assessment. Because data is without inherent meaning and appropriate value, exclusive reliance on Net-D cannot establish value handles to data to measure the support data provides to mission operational decision making. As a result, subsequent effective damage assessment is defeated before it can begin.

In terms of performing effective damage and mission impact assessment, the Air Force is finding that its information policy and doctrine do not translate well into Net-D implementation. Thiem's case study research (2005), when coupled with the interview data of this research effort, shows that reliance and focus on the technical assessment only is causing current damage assessment efforts to fall short damage assessment. The interview data provided evidence to an implication of Thiem's case study research on Air Force damage assessment that current damage assessment efforts are not actually assessing damage. Instead, agencies are simply producing technical and economically focused metrics that are of little use in understanding the full effect of the incident (Thiem 2005, pp. 34-35).

Net-D is a highly effective implementation of technological security policy, but it cannot continue to be solely relied upon to provide all aspects of cyber protection and security. Net-D must be implemented in support of a cyber protection scheme that

recognizes and understands information asset value protection. The current exclusive reliance on Net-D cannot support this effective damage and mission impact assessment. The Air Force must encompass an effective risk management program that allows it to identify, valuate, and document its information assets. The clear area of responsibility of technologically focused network security can be passed back to the Net-D function to protect these critical information assets that exist within the infrastructure.

Lack of Effective "Cyber" Risk Management.

Virtually all contemporary security planning methodologies include risk management as the foundation for a successful information security program. The Air Force understands the importance and benefits of risk management and employs risk management processes throughout the various aspects of its operations to achieve a high level of operations security. However, it fails to perform *effective* risk management of its information assets. The risk management that is accomplished is driven by the technology focused approach to cyber security.

The Air Force implements what Soo Hoo calls scenario-analysis risk management techniques (Soo Hoo 2000, p. 11). This form of risk management is very limited in scope. The Air Force tends to focus on those mitigation steps for those vulnerabilities identified explicitly identified through scenario. The Air Force is perpetually concerned about the damage and mission impact that may be caused a *zero-day* exploit. Since the Air Force does not deliberately assess cyber risk in terms of assets and value, it is discovering that it is largely blind to mission impact determination until after the impact is manifest. As the interviews and existing case study research (Thiem 2005) data demonstrate, the Air Force is finding damage and mission impact assessment exceedingly

difficult to perform effectively since organizations do not understand the assets owned and what these are worth to the organization's mission. An effective risk management program allows an organization to develop this understanding.

The Air Force is failing to implement a deliberate and effective risk management program. In practice, technology is the center of value against which degrees of security controls are established. When an incident occur, damage and mission impact cannot be done with accuracy and effectiveness. The problem created by putting technology exclusively at the center of risk management is analogous to only accounting for the hangars on a flight line and ignoring the aircraft and assets within. When catastrophe occurs, either through attacks or accident, and the hangar is lost simply reporting the cost of the damage to the hangar building provides the commander little understanding to the impact the attack had on mission capability. The commander must know what and how many aircraft and support assets were lost to understand the impact of the incident on mission capability and his ability to support the air campaign.

By implementing a risk assessment practice that focuses exclusively on technological assets, and fails to deliberately consider cyber information assets within the organization, the Air Force is simply inventorying hangars and ignoring the mission assets within. The failure to effectively perform asset-focused risk assessment is the chief contributor to the failure of damage assessment efforts, and is confounding subsequent mission impact assessment efforts.

Lack of Information Asset Documentation.

One considerable problem mentioned by interview respondents as impeding cyber damage assessment is the lack of usable documentation of cyber information assets used

within an organization. Interview data revealed that many Air Force commanders rely on *commander's programs,* such as the Operations Security (OPSEC) program to identify document critical information resources within the organization organizational structure. The OPSEC program was not designed for this task and cannot accomplish such an objective. The current implementation of the OPSEC program does document the organization's critical information resources, but it excludes most information in the cyber domain, other than information GWOT-focused information such as personal information published on a publicly accessible web page. There is no valuation of the assets collected in any way that is meaningful for cyber damage and mission impact assessment.

System accreditation documentation, another existing documentation of systems on Air Force networks, tends to be heavily focused on the technical aspects to be usable in cyber damage and impact assessment activities. Several interview respondents noted that this accreditation documentation is of little use in determining damage and mission impact after a successful incident. As a result, the Air Force has fallen short of establishing a platform of documentation to assist both the incident responder and information owner to damage and impact determination.

Current Attempts to Assess Damage and Mission Impact.

The Air Force's approach to cyber security is also directly driving it approach to damage assessment. This approach to cyber asset damage assessment attempts to determine the damage caused by an information security incident through assessment of technical impact to systems and/or infrastructure. It is fundamentally limited in its ability

to measure impact in a value-focused manner and is finding that it does not possess the ability to accurately measure mission impact following an information compromise.

Figure 9 is a conceptual graphical of how existing incident response process currently works and how damage assessment is determined and communicated within USAF networks. When an incident occurs and is detected, the IRT is dispatched to investigate the incident as shown in step 1. The incident process conducted by the IRT will focus on investigation, remediation, restoration, and a preliminary damage assessment as shown in step 2. The IRT team will work with the system owners in an attempt to determine the impact of the incident. In many cases, the system owners are not fully aware of all of the information assets that are contained within the system. This is due, in part, to the dynamic nature of information systems and the fact that information assets are often deposited on (or deleted from) a system without the explicit knowledge of the system owners. Next, a preliminary assessment of the incident is reported through AFNOC NCD to all affected sites as shown in step 3. In this high-level example, the report consumers are all those agencies that have a vested interest in receiving the incident report. Current damage reporting is integrated in the narrative of incident reporting consists mainly of tangible technical metrics (loss of availability of data and the man-hours required to remediate the incident). A subjective operational impact assessment may occur based upon the relative understanding the system owners have about the use of data affected by the incident. In most cases, this understanding is very low and incident responders are force to make a “best guess” based on their interaction with the system owners. As a result mission impact assessment is, for all intents and purposes, currently an unattainable goal due in large part to the lack of documentation of

the information assets on the system and identification of organizations that depend upon the information.

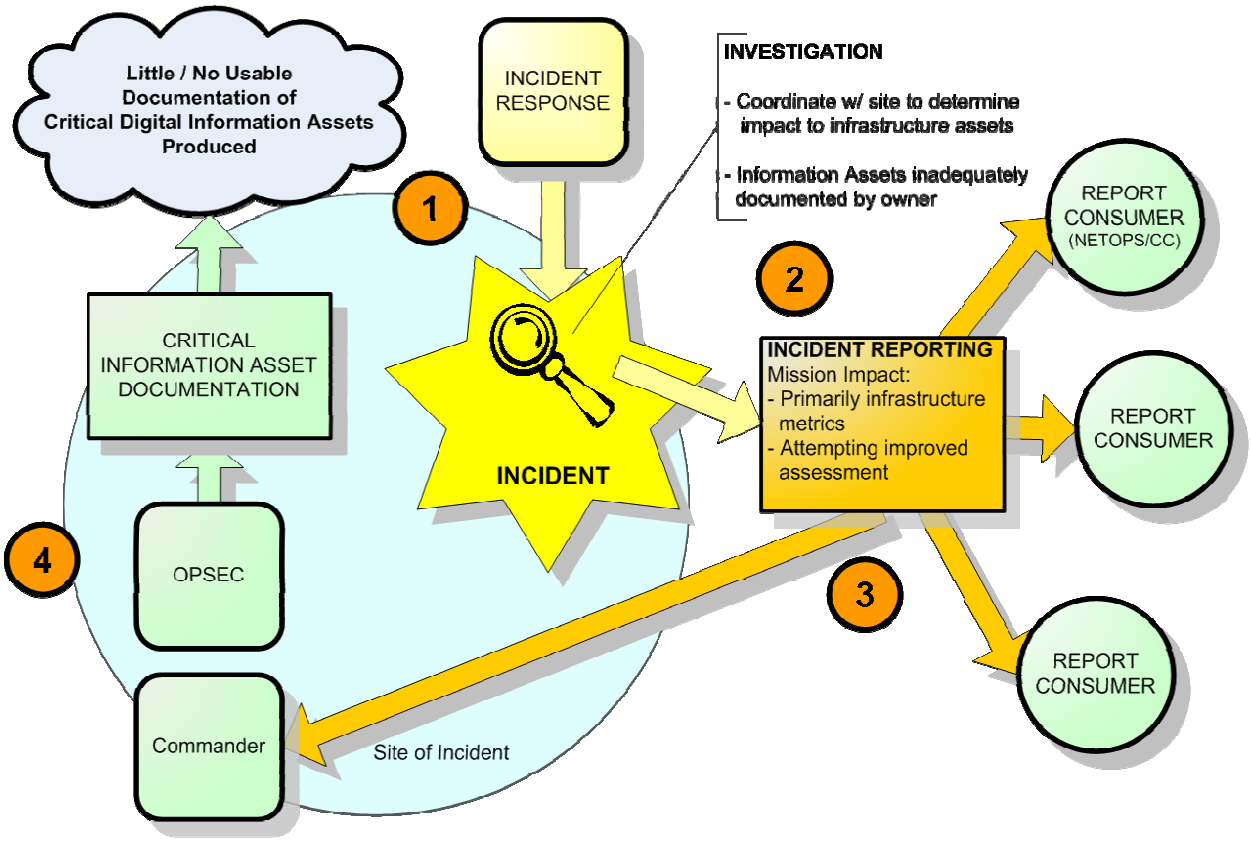


Figure 9. Current Incident Response and Damage Assessment on AF Networks

Step 4 illustrates this disjoint between the OPSEC program and cyber security efforts. As previously stated, the OPSEC program in its current is not designed to provide a commander any mapping of cyber information assets to operational or mission impact. There exists no other program or initiative in the Air Force enterprise to ensure identification, documentation and relative valuation of information assets that support mission operations and reside within the Air Force network infrastructure.

When an information incident occurs, the Incident Response Team is forced to conduct a mission impact assessment with little or no documentation that shows how the information supports the organizational mission. As a result, the primary assessment is based upon economic factors (remediation and recovery costs) and availability. Subsequently, an effort is made to identify and quantify the impact by contacting a representative within the information owner's organization. Unfortunately, this often leads to a subjective assessment and unreliable assessment of impact.

Scenario Illustrating the Current Approach.

To illustrate the impediments to damage assessment introduced by the currently employed approach to cyber protection, consider the following notional example based on actual events on Air Force networks where network defenders investigating suspicious activity have confirmed the compromise of multiple passwords to military systems. The systems are multi-function, but bear trust relationships with systems that are known to be critical to the organization's mission. The incident response team (IRT) determines that at least one password has allowed administrator access to the system; and the mission critical systems were accessed numerous times. All findings, including time of access, information accessed, and other important information, are reported through the standard reporting chain, and the commander at the site of the incident is included. The commander requests more information from the IRT regarding how the incident affects his mission. The IRT is unable to provide this assessment as there is no documentation of how the information provides value to the mission. As a result, the commander may decide that since his system's availability is intact, no action is necessary. The truth,

however, may be that the confidentiality of a planned operation was breached which undermines the OPSEC of the mission. As a result, the mission may be jeopardized and materials and lives exposed to unnecessary risk since the commander cannot be provided with a clear picture of the battlespace that enables him to understand the impact to is own mission capability.

Synthesis of Research Data and Investigative Research Questions

This section will address the investigative research questions and discuss the research data in terms of these questions. Each section will discuss how the data supports or weakens the investigative research questions.

Investigative Research Question 1.

The first research question asked:

R1. How can the damage resulting from a successful cyber attack be effectively measured?

This research has uncovered substantial data from literature review, existing case study research, and interviews to indicate that the current damage assessment methodology is inefficient at best, with non-validated damage assessment procedures being implemented piecemeal in various pockets of the Air Force enterprise (Thiem 2005, p. 43). Despite the Air Force implementing damage assessment and reporting command and control through standardized guidance (AFI 33-138 2004), there are still many problems as evident from the interview data.

The Air Force is attempting measuring damage in technical and financial terms, although these damage assessment metrics note have been proven beneficial to the

commander seeking to understand impact to his/her mission after an incident. The interview data of this research directly supports the findings of Thiem's research (2005) that damage assessment is an inherently technologically focused activity being conducted ineffectively throughout the Air Force enterprise.

Understanding Damage Assessment.

Damage assessment, mission impact assessment and mission impact reporting form a chain of dependent activities. Conceptually, one activity cannot be accurately performed without successful completion of the prior activity (see Figure 10 below). Cyber damage assessment must set the stage for mission impact by determining damage to the asset on which the mission depends. The damage is in terms of value loss. In other words, *damage assessment must assess damage*. In the literature review, damage was defined as a loss in value or usability in an asset (Oxford, 1986). Analysis thus far has shown that a failure to accurately perform damage assessment confounds any effort to perform mission impact reporting to the operational decision maker.

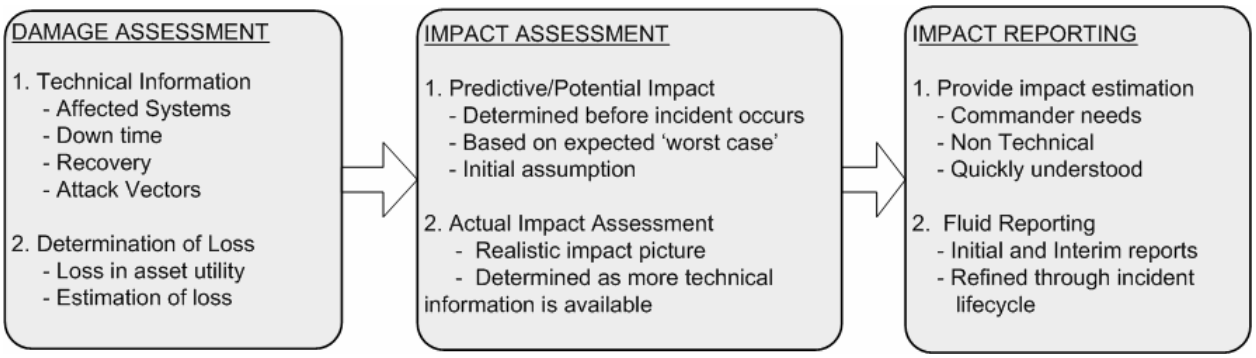


Figure 10. Damage Assessment to Impact Reporting Chain of Dependency

The previous statement is true because mission impact reporting is at the end of a chain of interdependent processes. The mission impact assessment is failing because of

the focus on the technical aspects of damage assessment. Air Force damage assessment is conducted in a disjointed manner and in many cases is limited to technical reporting without actual damage assessment being performed. Damage in terms of value loss is difficult to measure since the Air Force risk management program is a scenario-focused scheme that introduces limited scope to risk, and very little deliberate determination of asset value. In all cases, the central asset of damage assessment efforts is technological and which holds only a single dimension of value to the organization; loss of availability. However, as the research data demonstrates, the failure to understand the system-to-mission relationship is rendering even this simplistic, single dimensional form of damage assessment ineffective. The chain of dependencies must be corrected for mission impact assessment to be possible.

Ideal Cyber Damage Assessment.

Cyber damage assessment methodology must include a mechanism that provides a reasonable estimate of loss in the value of an organization's asset. This statement holds several important implications. It implies that an asset is something that holds value to the organization. Since damage is defined as a reduction in value or usefulness of the affected object (Oxford, 1986), effective damage assessment methodology must assess any reduction, or loss, in the asset's value. This, in turn, implies that effective damage assessment must also measure value loss in the *correct* asset in order to produce metrics that are relevant to the organization's mission. Such assets must directly support the organization's mission and the value of the supporting relationship must be understood by the asset's owner.

This research has found that Air Force organizations are not looking at the right assets for damage assessment, due largely to a failure to recognize what assets support the mission. Interview data and literature both support the strong focus that the Air Force maintains on technology over its information. The interview respondents cited a prevalent failure to understand how systems processed information that supported the organization's mission. The focus on technology has blinded organizational understanding of what assets are owned and how those assets contribute to the mission. Moreover, the interview data shows that this focus on technology prevents the understanding that the asset not simply the affected system, but it is the information processed by the system that supports the organization's mission. The literature review and interview data support the concept that the asset's value lies in the relationship between this information and the mission.

Additionally, the case study of damage assessment on Air Force networks revealed that the focus on damage assessment was exclusively on technical assessments, and in some cases a lack of understand of *why* damage assessment is being conducted (Thiem 2005, p. 35). There is no indication that an assessment of damage in terms of value loss is being conducted. This observation is supported by the interview data of this research effort in which every respondent discussed some aspect of the meaningless mission impact assessment metrics consisting of exclusively technical reporting from the Tier 3 custodians. If no damage is assessed in terms of utility value loss, mission impact assessment becomes even more difficult and less accurate. Indeed, one of the common themes among the interview respondents in this research effort was that the focus on

technical issues was producing meaningless damage assessment metrics that prevented mission impact assessment.

Ideal cyber damage assessment depends on the identification of the *correct* assets and an understanding of the *value* these assets maintain in the organization. Ideal damage assessment, therefore, is explicitly dependent on the identification and documentation of the information asset *before* the incident occurs. This documentation must account for the assets value in terms of mission relationship, its key attributes and containers, and an explicit mapping to the mission which indicates potential mission impact if the asset is lost or damaged. Value must be expressed in some way that is relevant to the organization. Literature review data supports that the value of information lies in its utility to the organization (Buffet, Scott, et. Al. 2004, pp. 80-81; Morrison and Cohen 2005, p. 34). In organizational decision making where mission is not motivated by economics, such as military operations, the value of the asset must be expressed and understood in terms of utility-based value estimation. By identifying the correct asset and understanding its relative value before an incident occurs, damage assessment then becomes possible. More importantly, identification, valuation, and documentation of the asset and it mission relationship opens the door to mission impact assessment.

This allows the information owner to work with the incident responder's technical assessment to understand the damage to the asset in terms of estimated value loss. Since documentation of the asset's key attributes exists, the asset owner can now map the technical report assessing adverse effects against the organization's *systems* to the assets on the systems. The documentation further assists the owner and incident responder in determining how the asset supports the organization's mission. The asset owner can

readily understand the relationship between the system and the asset. Any estimated reduction to the asset's utility value may be assessed as damage in terms acceptable for translation to mission impact assessment.

Investigative Research Question 2.

The second research question was:

R2. How can such damage be mapped to impact to an organization's mission capability?

The previous section established that once the correct assets are identified and their value understood before an incident occurs, accurate damage assessment may be accomplished. Damage to mission mapping depends on accurate pre-incident determination and documentation of asset-to-mission relationships. If accurate identification and documentation of the organization's assets, asset value in terms of mission operational utility, and key asset attributes is accomplished before an incident occurs, a great stride is made towards mapping the asset to a potential impact on the mission if the asset is damaged.

The chief theme revealed in the research data was an exclusive focus on technology produces an organizational environment where the relationship between a system affected by a cyber incident and the organization's mission is misunderstood. Such a failure to understand the critical mission relationship frustrates attempts to assess both damage and mission impact in the affected organization. Several respondents cited the lack of any documentation to assist the Tier 3 damage assessors in understanding this relationship. The establishment of such documentation facilitates a new ability to perform both the foundational cyber damage assessment activities and more important

mission impact assessment activity. Therefore, pre-incident documentation of the asset, its value, and its mission relationship lift the fog which currently exists. With a clearly documented mapping between the asset and the mission, cyber damage to mission impact assessment becomes possible.

Another key finding in the interview data was the fog produced by this exclusive focus on technological assets and lack of documentation was the misunderstanding of ownership. The literature review Stevens discussed the many problems associated with failure to establish and understand ownership (Stevens 2005, p. 30). The research data revealed evidence that organizations did not understand ownership roles of the system and the associated damage assessment processes. These agencies depended on the Tier 1 agencies to determine damage and mission impact assessment. However, only the asset owner has the perspective to understand how the mission is impacted when the asset is damaged. Establishing and documenting explicit ownership of the organization's assets facilitates both damage assessment and mission impact assessment by mitigating ambiguity about the asset attributes and ensures that the entity with the appropriate perspective can work with the Tier 1 agency to establish an effective mission impact assessment.

Damage assessment mapping to mission impact may be accomplished through the foundational activity of identifying and documenting the organization's assets and appropriate attributes *before* an incident occurs. These attributes must include at minimum, the asset owner, the asset's value in terms of mission relationship, and such information as the asset's location. By doing so, the first key activities of damage and mission impact assessment may be accomplished.

Investigative Research Question 3.

The third investigative research question was:

R3. How must this assessment be reported to the decision maker to maximize the quality of the assessment for use as decision input?

Mission impact reporting is the summit of all damage and mission impact assessment activities. Appropriate and effective reporting can provide the commander with an increased situational awareness of potential and actual impact to his/her mission following an cyber incident that may lead to improved battlespace decision making through decision superiority (AFDD2-5 2005). However, literature review (Bowman and Moskowitz 2001, p. 775) has shown the usefulness of the reporting data is only as good as the effectiveness of the preceding assessment process. Additionally the information must be of decision-making quality in terms the decision maker can easily understand (Jensen 2005, p.56; JP 3-13, 2006: I-3).

Mission impact reporting inherently assumes all previous supporting activities have been accomplished effectively and accurately and must be approached from an operational perspective. Technical issues relating to damage assessment must be translated into a report that is free from technical details. Mission impact assessment reporting *must* present information that is *relevant to the commander's needs* and in terms of the commander's frame of reference. The mission impact assessment report must be simple to understand quickly with minimal technical information. It must produce an immediate understanding allowing the commander to quickly assess the impact information as it relates to his/her mission.

Literature review and interview data has shown that the primary guidance for such reporting (CJCSM6510.01 2006) does not explicitly provide such a reporting format that is free from the ambiguity that results in overly technical reporting. But as previously stated JP 3-13 (2006, p. I-3) does provide a generic framework for the establishing the *quality* of information that must be included in mission impact reporting. If the quality criteria are used as a standard for developing report content a good start is make towards effective reporting. To ensure that the report is populated with assessment information that is relevant to the commanders needs, asset owner involvement in impact assessment and reporting is essential.

Timeliness is also a critical issue to ensure the appropriate decision maker gains situational awareness in appropriate time frame. Ideally, report distribution should be automated through some centralized reporting system to ensure all organizations, such as Tier 1 Netops functions, and ordinate agencies are aware of the mission impact resulting from the incident on the enterprise networks.

From the first phase of asset identification to the final phase of mission impact reporting, the needs of the operational decision maker must be at the forefront of all activities. Only by maintaining this operational focus will information, rather than technology, become the evident asset for mission, and its value realized. By doing so, the fog that obscures the relationship between information asset, system and mission is lifted and true cyber damage assessment and mission impact assessment becomes possible.

Chapter Summary

This chapter presented and analyzed data collected through the interviews, existing case study research on damage assessment practices on Air Force networks, and extensive literature review. The interviews focused on understanding the problems with current mission impact assessment activities. The literature review and case studies examination analyzed data relating to the Air Force's approach to risk assessment and damage assessment. The key finding is that the foundations of all network defense activities are so exclusively rooted in the technological focus that accurate mission impact assessment is not currently possible. Mission impact reporting is at the end of a chain of interdependent processes. It is failing because the preceding steps are failing. Damage assessment is conducted in a disjointed manner and in many cases is limited to technical reporting with not real assessment of damage in terms of value loss. Value loss cannot be measured since the Air Force risk management efforts do not deliberately identify and valuate cyber assets.

This chapter answered the research questions after building an understanding of why current damage and mission impact assessment is not working efficiently. Damage from a successful cyber attack may be measured effectively only if the value of the asset if known before the incident. Damage assessment must consist of both a technical assessment *and* a damage assessment that estimates value loss. Mission impact assessment depends that damage assessment is successful and accurate. Both damage assessment and mission impact assessment explicitly depend on accurate asset identification and documentation prior to the incident. Mission impact reporting is the end goal of all damage and mission impact assessment activities. It depends on

successful and accurate accomplishment of the previous activities and must provide the results in a timely and clear manner to allow the decision maker to make smart and timely decisions based on the mission impact report information.

V. Conclusions and Proposals

Introduction

The previous chapter discussed the finding in current Air Force implementation of damage and mission impact assessment. The chapter also provided answers to the research questions by discussing how damage assessment can be translated to mission impact and clearly reported to the organizational decision maker.

This chapter discusses conclusions of this research regarding improved defensive damage assessment methodology. The first section of this chapter presents foundations for improved damage and mission impact assessment. The second section proposes an improved conceptual methodology for defensive cyber damage and mission impact assessment.

Foundations for Defensive Cyber Damage and Mission Impact Assessment

Defensive Cyber Damage and Mission Impact Assessment (CDA-D/MIA) is a system of interdependent activities that allow an organizational decision maker to understand the mission impact resulting from a successful cyber incident. The methodology attempts to help an organization identify its critical information assets in such a way that effective mission impact assessment and reporting is possible. This research effort has determined that current attempts of both damage assessment and mission impact assessment are unsuccessful due to a number of independent failing that prevent its effective implementation for a number of reasons. This section will discuss essential foundational principles that establish an *improved* methodology.

Information Production, Consumption and Ownership.

The literature review discussed traditional concepts of information ownership, custodianship, and information users. Understanding these respective communities of responsibility regarding information is extremely important for the foundation of damage assessment. The information owner is responsible for identification, definition, valuation, and documentation of all information assets owned. Asset profiling must be accomplished by the information owner since only the owner maintains a perspective to understand how the information is used to support the organization's mission and its relative value. Assets must be identified, documented, and profiled *before* an incident occurs.

In the best of conditions, information production, ownership, and consumption are easily and frequently confused, and in many organizations information asset ownership is assigned without due diligence to ensuring the owner can accomplish the assigned ownership responsibilities. Ownership must be assigned correctly or any benefits are negated. The assigned owner must both understand the responsibilities of ownership *and* possess the authority to perform ownership duties.

Ownership must not be confused with production. In many organizations, the producer and owner may be the same person if the information asset is produced within the organization. In a large enterprise, the information producer may exist outside the organization that holds the information as a valued asset. This is especially true on military networks.

Tangible Ownership.

In a business organization, it is likely that information is produced somewhere *within* the organization's boundaries. In such a case, the information producer and information owner may be the same. It may be reasonably expected that since they reside within the same organization they are subject to the same organizational policies governing information and information asset protection. This situation creates an opportunity to create a *tangible* assignment of ownership.

The *tangible owner* possesses reasonable assurance that the information asset will be subject to the consistent information policy and guidance as established within the organization. Additionally, the tangible owner maintains a reasonable relationship with the information custodian since, as with the information producer, both operate within the policy environment of the same organization. Furthermore, since the tangible asset owner and asset are *within* the same organization, the owner is in a position to place a value upon the asset relative to its contextual worth to the organization with reasonable assurance that the relative value of the information asset is sustained throughout the organization. Tangible ownership can only exist in organizations where information assets do not cross organizational boundaries.

Relative Ownership.

In a large enterprise, such as the military, tangible ownership is impossible to achieve. Military operations rely heavily on information assets produced beyond the boundaries of the organization, service, or even the nation of the information consumer. On military networks, the traditional role definitions information producers, owners, custodians and consumers are obscured as traditional concepts of ownership become

relative to the individual needs of widely diverse organizations within the same enterprise. Asset ownership gains a new fluidity, and becomes relative to the contextual value within an organization. The same asset will have widely differing values and security requirements as it moves from organization to organization throughout the enterprise. Assignment of a single owner is impossible in this case, therefore ownership is *relative* to the organization.

To illustrate this concept, consider the following scenario. An organization receives intelligence information input from multiple external organizations, services, and allied nations. External information producers may classify the information at the point of origin, but because the external producer has no perspective of how each consumer organization will use this information within the context of each mission, definitive value for the information cannot established. Therfore, classification can only serve as a baseline value for the asset. As the information enters the organization and the organization finds that the information is useful to its mission, the information becomes an asset to the organization. The organization, therefore, may store and use the information. At this point, the organization becomes more that just a consumer of the information asset. Now the organization is a *relative* owner of the asset.

In this way, *relative ownership* resembles tangible ownership, local to an organization for the purposes of risk management, security controls, and even damage assessment. As with the tangible owner, the relative owner is responsible for identification, documentation, and valuation of the information asset. However, each organization within the enterprise that uses the asset may realize asset value differently in

the context of its mission usability. Each organization, therefore, bears a relative ownership to the asset within the context of their organization.

The concept of relative ownership is extremely important to establishment of an effective cyber damage assessment model in a large and diverse enterprise, such as the DoD. Relative ownership implies that *the buck stops here* for determining asset value. Relative ownership allows each organization to look within itself to identify, document, and valuate the critical information assets that allow it to maintain daily mission operations. For the purposes of this research, the term information ownership implies relative information ownership to more easily deal with information ownership and damage to information assets *local* to the organization in which the incident occurred.

Measuring Cyber Damage as Value Loss.

This research has concluded that traditional methodologies for assessing cyber damage are not suitable for use on military networks. Traditional methodologies tend assess damage in terms of economic loss and produce reporting constructs that are not adequate contributors to decision making in organizations not explicitly profit-driven. .Additionally, this research determined that Air Force damage assessment efforts do not effectively measure damage in terms of value loss. This is one contributing reason why current damage assessment cannot facilitate impact assessment. The other contributing reason is a failure to understand value in terms that are relevant to an organization such as the military. Without establishing relative value, damage cannot be assessed. This section proposes a conceptual method for establishing value and assessing subsequent damage resulting from an incident.

Establishing Value for Information Assets.

Determining the value of information is a complex task due to its innately intangible qualities and contextual derivation of value that thwarts attempts to assign a definitive value to information assets in many models. Understanding information value as a reflection of the relationship it presents in supporting the achievement of *organizational mission goals* is critical.

The value of information is contextual; it is derived from its utility within a given organization. Utility is an intangible quality that is extremely difficult to quantify because it is dependent on the context in which the owning organization uses the asset in achieving its mission goals. The value of information may deviate greatly from one organization to the next due to context. Consider for example, live unmanned aerial vehicle (UAV) feeds providing real-time battlespace information may be broadcast across a classified network. Personnel in the finance organization may access this information at any time to see what's happening. As interesting as the feed may be to the personnel in the finance unit, the UAV feed holds little or no value to the mission of the finance organization. If a cyber incident impairs the live feed, there is no immediate impact to the mission of the finance organization. Therfore, the feed holds little value to the finance organization. However, the information holds great value to the commander in the Joint Air Operations Center (JOC) making mission decisions based on the information provided through the feed. The information is the same to both, but the value of the information is contextual and driven by utility. The problem encountered is how to create a value handle to measure this value; and determine loss when the asset is compromised.

The greater the utility of the information asset to making decisions supporting the mission goals the greater the instrumental value the asset presents to the organization. As more decisions can be made on the information asset supporting the organization's goals the more the asset's value increases. As this value increases, the tangible aspects of measurement tend to decrease (see Figure 11 below).

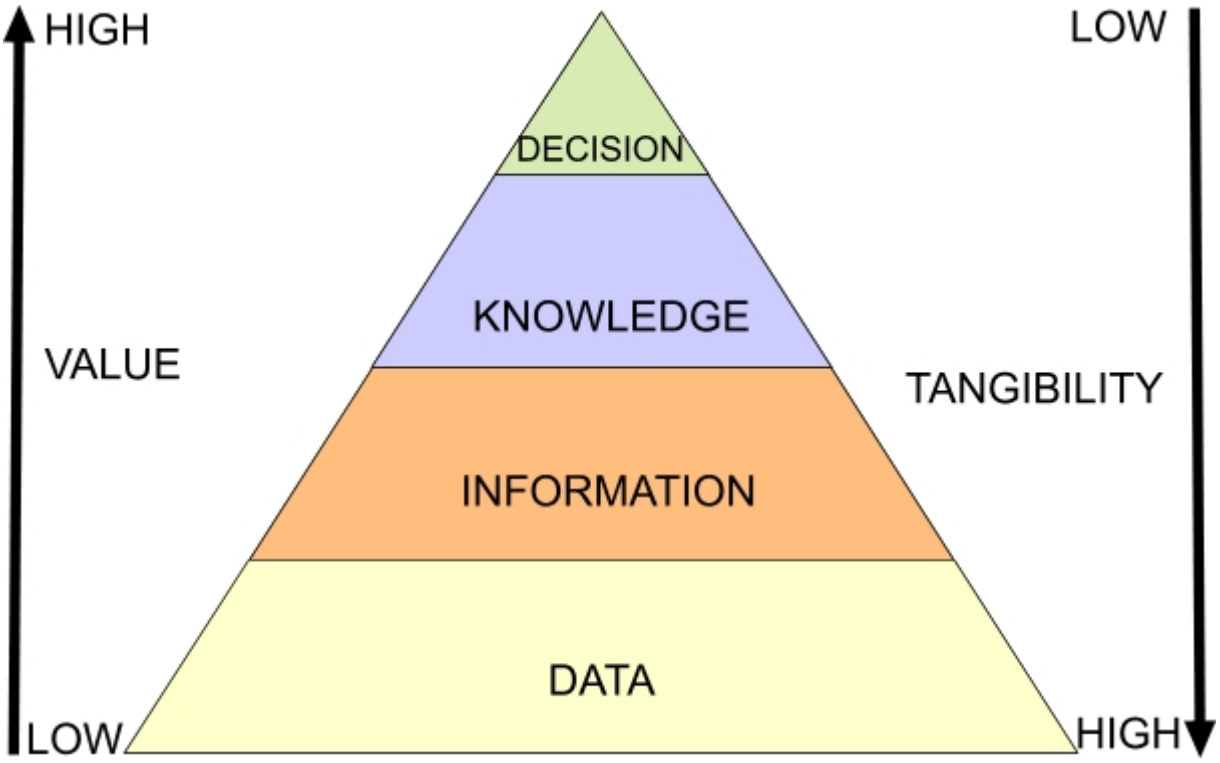


Figure 11. Information Value Hierarchy

To assess damage to information and the associated mission impact, however, some approximation of value must be determined prior to incident occurrence. On military networks, classification is an intial baseline, but it is not a sufficient measurement of potential or actual value. Therefore, a new model for value assignment must be devised to assign a *handle* to represent the instrumental value the information

asset holds relative to its support of organizational mission operations. When doing so it is critical that focus remains on the information asset as the foundation on which specific mission operations rest. By approaching asset value determination from a mission operations perspective, the complexity of identification and valuation may be reduced by approximating it value in relation to its value drivers.

Asset Value.

Value is an abstracted concept and there are many things that go on *under the hood* to establish the concept of value, and it is frequently confused with its unit of measurement. It is worthwhile to briefly discuss value as it relates to damage and mission impact assessment, because understanding how to determine value is essential to understanding how to determine damage.

The conclusions of this research assert that an asset possesses value in two distinct ways: *potential* value, and *actionable* value. Potential value represents the absolute value that an asset may *hold* for an organization, real or theoretical. Potential value tends to remain constant so long as its value driver remains constant. Actionable value represents the degree in which the value is presented to the organization. Actionable value is based on the organization's ability to *utilize* the asset for its needs at a given time. Where potential value is relatively constant in regards to its relationship with its value driver, actionable value is relatively fluid and is readily influenced by external factors. For example, an asset with high utility by critical mission processes may be unavailable as the result of a server failure. The asset's potential value remains constant—it is still an important asset to the organization—but the actionable value is

diminished. Since the asset's ability to be used is diminished, the value it provides is diminished for the duration of the reduction in utility.

This concept is important since military operations depend upon these values differently in operations across the strategic, operational, and tactical domains of operations. The strategic domain is primarily concerned with the asset's *potential* value to establish predictive understanding of potential mission impact. In the operational and tactical domains, however, mission operations depend on the organization's ability to effectively use all the constructs of the information asset, therefore relying upon the asset's *actionable* value. The asset's value must be established before the incident occurs and by necessity, through an asset-focused risk management methodology which facilitates asset identification and valuation. On initial valuation the asset's potential and actionable values are presumed to be the same. To assign value to the asset, however, there must be value constructs established to which value may be assigned and damage may be assessed. These constructs are discussed further below.

Classification as a Baseline Value Construct.

All information stored on its networks is assigned classification through a standard system for classifying, safeguarding, and declassifying national security information (EO13292 2003). The classification is established at the point of production in terms of value to national security rather than value to a specific organization's mission. However, this classification is maintained across organizational boundaries regardless of an organization's mission. A system must be accredited and classified at the highest classification level of the information processed on it. Thus, *all* information stored or processed on the system must be assigned a classification level equal to that of

the system. As a result, there can be no guarantee that the classification is a reflection of the asset's value to the individual organization making classification only suitable as a baseline for establishing asset value.

Utility as a Contextual Value Driver.

Information asset value is contextual, since its value is in its support of the organization's accomplishment of its mission goals through operational processes that depend on the information asset. Remember that contextual value is the most important component in information asset valuation, and derives its value through its degree of utility in supporting the organization's mission. Contextual value allows the same asset to be worth more or less from one organization to the next as its utility changes. The more usable the asset is, the greater its contextual value. The greater the utility to a process critical to the organization, the more critical the asset becomes. This also means that when something occurs that affects the utility of the asset in its relative ability to support mission goals, its contextual value is affected. Such a change could be the result of a shift in the organization's mission that makes the asset less useful. More often it may be the result of an incident that affects one or more of the asset's contextual value constructs.

Contextual Value Constructs.

The model below proposes an asset value model in which assets can be assigned value based on their criticality to the mission. Valuation must be done in the pre-incident stage of the strategic operating domain of the CDA-D/MIA model. CDA-D/MIA domains of operation will be discussed later in this paper. Valuation of the asset constructs is a critical component in the success and effectiveness of the CDA-D/MIA

methodology. This model allows a discrete value to be assigned to the qualitative relationships between the asset and the mission it supports. These relationships are identified in the model through asset constructs which model the utility bindings of the key areas of support for the organization's mission (see Figure 12 below). Remember that this support for the organization's mission is realized through layers of support of information processes which support mission processes and ultimately the organizational mission. The constructs of the contextual value of information are mission binding, age, and state.

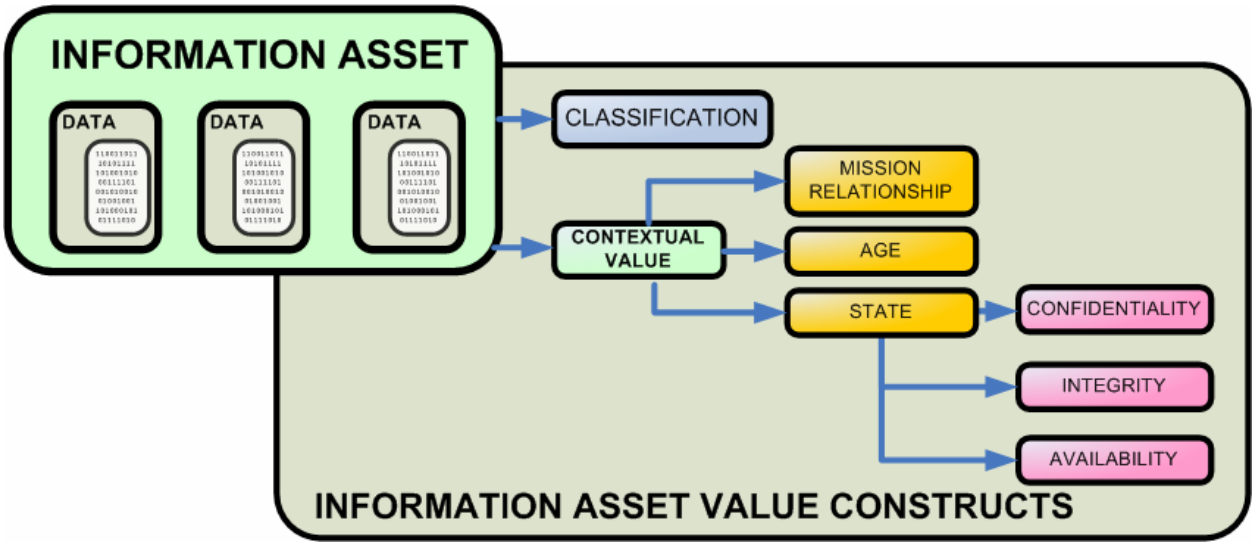


Figure 12. Information Asset Value Construct Model

The Mission Binding Construct.

Mission binding is an assessment of how closely the information asset is bound to the organization's mission through its supporting information process. An asset that is closely bound to an operational process is assigned a relatively high value, especially if the operational process itself is critical to the organization's mission. Therefore, the

criticality of the supported process and the strength the relationship between the process and the asset comprises the value driver for the asset's mission binding construct. The nature of this relationship enjoys a relatively greater degree of permanency in comparison to the other contextual value constructs, especially those sub-constructs under the state construct discussed below. Mission binding is qualitative in nature.

The Age Construct.

Age is a concept common to all lifecycles. As information ages, it's relevance to the organization may change. This construct could conceivably be call timeliness, but since the degree of relevance reflected in this construct is function relevance over time, it is more appropriately called age. Some information assets may possess a more volatile age construct than others. The value of the age construct of a weather report will potentially alter more rapidly than the age construct of electronic patient records. An asset which ages beyond its relevance will see a reduction in utility. Assessing the value of this construct is arguably more useful in those assets that age at a more gradual rate. The value of this construct is also qualitative.

State Constructs.

State is the most fluid of an information asset's contextual value constructs. The state construct refers to the state of the *Confidentiality, Integrity, and Availability* (*CIA)* model of information quality and reflects the asset's state of confidentiality, integrity, and availability. Each organization may place a greater or lesser value on each of these constructs depending on how the asset supports the particular mission process. Certain processes may depend on the state of a certain construct to be maintained more than the others. For example, some information assets, such as secrets, may not need to be

immediately accessible, but unauthorized exposure could be devastating to the organization's mission capability. Others, such as medical prescription information stored in a system depend on the maintenance of the integrity over confidentiality and immediate availability.

An information incident can affect the state of the information asset causing it to be of less value to the information owner. During initial valuation, it must be assumed that the state constructs are intact unless there is reason to believe otherwise. Like the mission binding construct, the constructs which comprise the asset's state construct are qualitative estimations of the value the asset provides to the organization is achieving its mission goals.

Damage and Value Loss.

Loss is value reduction in the asset. However, value loss is not necessarily the result of damage. Value loss can result from either external *or* internal influences, such as organizational mission changes or incidents that affect the relationship maintained between the asset and the supported mission processes, or internal factors such as life cycle issues that diminish the asset's relevance to the mission. Value loss can occur from information life cycle issues, where the asset outlives its relevance to the organization, thus experiencing value reduction. If the organization's mission changes, the asset's value may decrease if it is not as critically bound to the organization's new mission.

Damage is something more specific. Damage is the result of an *incident* that reduces the asset's utility to the organization; generally and most frequently affecting the asset's context value constructs. Damage is always the result of an external influence on the asset's value.

This research is primarily concerned with damage. However, both damage and general value loss are reductions in value, so it is important that a methodology for damage assessment is also able to recognize other forms of value loss in the organization's information

Value Loss in the Mission Binding Construct.

Generally speaking, the mission binding will remain relatively constant so long as there is no change in the value driver. A change in the organization's mission may cause a cause a change in the value of the asset if the supported process becomes more or less critical to supporting the organization's mission. Another factor that could influence the mission binding is age.

Value Loss in the Age Construct.

As previously stated, an asset that has aged beyond its relevance is less useful for decision making. Since decisions are made upon information, the information must be timely and relevant to the situation to possess utility in decision making. If the information asset is no longer applicable its utility is reduced, with potential collateral impact to the mission binding construct.

Following with the previous example of age, consider that a weather report may be updated and revised multiple times throughout the day to provide the commander the opportunity to maximize the potential for improved mission decisions. Each successive report supersedes the previous as the previous ages beyond relevance to the mission.

Damage in State Constructs.

Because of the nature of state constructs, value loss will be experienced as damage. These constructs are not directly influenced through time or mission alignment.

Changes to the value in these constructs will come from some external influence or compromise. Therefore, such value change is damage. Each of the sub-constructs of state, confidentiality, integrity, and availability, can experience damage independent of each other, or collectively. Each holds in independent value that reflects the value state of the construct at the time of its valuation; presumably also its ideal state. An incident that results in any degree of value reduction in any one or any combination of the sub-constructs of the state constructs reflects a reduction in the utility of the asset for the duration until the asset may be restored to its pre-incident state. Again, keep in mind that discussion of loss in these sub-sections refers to reduction in the actionable value.

Damage in Availability Construct.

There are multiple avenues for a compromise of availability. Loss of availability can be caused by malicious activity, such as a Distributed Denial of Service (DDoS) attack against the information infrastructure, or non-malicious incident, such as natural disaster or infrastructure failure. Consider the following example of damage resulting in mission impact following from a compromise of information asset availability.

The air campaign is in its second day. One of the wing commanders supporting the campaign wants to know the wing's BDA for the previous day's missions; and specifically why he is attacking the same target for the third consecutive day. He calls the Director of Combat Operations (DCO) for BDA report, but is informed that an ongoing system outage is delaying access to the BDA reports. The DCO states that the cause of the outage is unknown at this time, but his Intelligence officers will be able to resume completion of the first phase BDA report as soon as the system is operational.

The Colonel on the phone is frustrated because he cannot get the information that he needs about the next day's missions.

In this scenario the critical information asset was unavailable to support the organization's mission. The availability construct was perturbed by a container failure, resulting in a degradation of the asset's actionable value. Damage in this case is realized since the asset is not available for use and the mission capability, or at minimum efficiency, is directly affected until such time the information asset is made available again. The potential value of the asset has not diminished. It cannot be acted upon, however, there the availability sub-construct's value is diminished reflected as damage to the asset's value until it is made available again.

Damage in the Confidentiality Construct.

Consider the following notional example that illustrates how a confidentialiy compromise can result in damage to the confidentiality value sub-construct that translates to mission impact. As the build up for impending operations to regain control of Fallujah begins, CENTCOM network defenders notice an increase in suspicious activity on MNF-I networks. The widely dispersed network and necessities of combat operations introduce delays in the incident response activities necessary to secure and investigate a cluster of potential root-level compromises on systems located somewhere on Camp Victory. Administrators and incident response personnel attempt to locate and secure the systems suspected have sustained Category I (CAT I), but are met with resistance from operators to shutting the systems down as they are mission critical. The suspected compromised systems operate for another 9 hours before being secured. In all the systems processed critical mission information for 36 hours after the initial notification

by CENTCOM network defenders of suspected root level compromise. Within 24 hours the number improvised explosive devices (IED) and other hostile actions on all convoy routes increased by three hundred percent, with at least two IED detonations causing multiple coalition casualties, including loss of life. This forced a change in movement time tables and routes. Forensic investigation revealed that two systems used for processing mission critical information had, indeed, been compromised at the root level. Both systems were classified systems that had been connected to an unclassified network, providing the intruders access. The intruders did not alter information on the system, but quietly accessed and retrieved large quantities of sensitive and classified information, including all convoy times and routes for the next several days. Since the impact of the confidentiality compromise did not immediately impact mission operations as with an availability compromise, the severity of the compromise was not understood until too late. As a result mission operations were affected, and human lives lost.

A breach of confidentiality is more difficult to detect than an availability compromise. The effects of confidentiality may not be immediately apparent, as in the above scenario, but this very fact may cause the impact to be greater. Some information assets, such as secrets, will suffer significant devaluation if known by another entity with the capability to exploit the information. When such a confidentiality compromise the asset experiences a actionable reduction in actionable value, since the secret is no longer a secret. Even if the decision maker elects to proceed with the asset to make a decision on mission operations, the value presented is still not equivalent to the its potential value.

Damage in the Integrity Construct.

The following notational scenario illustrates who damage to the integrity construct can result in mission impact. Recent weeks have borne witness to a growing number of network incidents, and MNF-I leadership is concerned about network operations and cyber security problems that have recently affected Multinational Corps – Iraq (MNC-I) mission operations. The MNF-I/J-6 has tasked the MNC-I/C6 to ensure that all units in the Iraqi theatre of operations provide owned and used IP ranges to 3d Signal Brigade to aid in more rapid isolation and location of system outages and suspicious activity. Unfortunately, not all units comply. CENTCOM network defenders watching both CENTAF and CFLCC intrusion detection sensors report new potential CAT I activity from systems on MNF-I networks. Although the IP of the suspected compromised systems are assigned to CENTAF at Balad Air Base, the system cannot be located immediately and the suspicious activity continues intermittently for three weeks. During this time, medical staff at Balad Air Base experience an unusually high number of anomalies such as patients being administered the wrong drugs or dangerously high dosages, incorrect blood type, and other life-threatening issues. When the suspected compromised systems are located and secured, compromised is confirmed. The intruders had intentionally altered patient medical records placing several patients in life threatening situations.

Like a confidentiality compromise, a compromise of information integrity may be difficult to initially detect and have severe impact to the organization's mission. Decision makers ultimately utilize information assets as the foundation of their decisions. Altering the information asset can force the decision maker to make a bad decision that negatively impacts mission operations. Integrity compromise degrades the actionable value, by the

degree of alteration and can be synonymous to an available compromise it the integrity violation makes the asset unusable. The potential value remains constant so long as the asset can be restored to its original state.

Establishment of a Relative Value Scale.

This research has established that value is the result of the asset's usefulness to the organization, whether utility in decision making or other, more abstracted mission dependencies. In any case, as this dependency increases, the tangible aspects that allow more simple value modeling in physical assets begin to diminish. Commonly measured tangible value qualities tend to focus on economic contribution of the asset, resulting in dollar-centric damage assessments that are of little use to the non-profit focused decision maker. In fact, previous research and existing models have shown that precise value of information cannot be determined with complete accuracy, or arguably even a high degree of accuracy. The best approach, therefore, is to develop the closest approximation of this value as it relates to the organization.

This research proposes that information assets possess two general areas of value: classification, which can only serve as a baseline value, and contextual value, which is the true indicator the support the asset has for the organization. Development of a methodology for cyber damage and organizational mission capability impact assessment require an information value model that can capture the qualitative estimation of the value an information asset holds to the organization; and present the measurement of this value with enough simplicity that it is easy to understand and work with. To meet this need, this research proposes a five-point value scale for value assignment to the

constructs of information assets in a non-profit driven organization such as the military (see Figure 13 below)

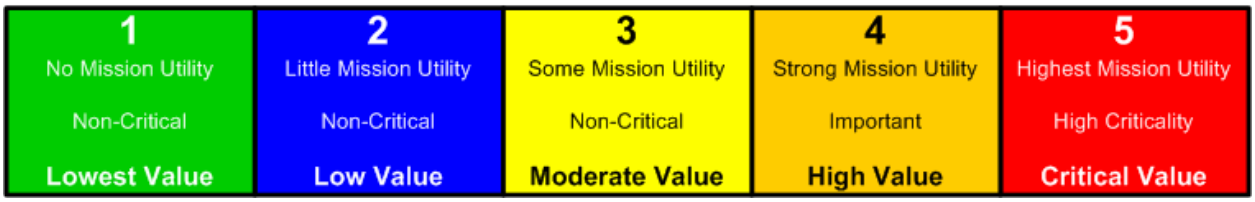


Figure 13. A Five Point Value Scale for Information Assets

This proposed value scale reflects the value of an information asset, through the value assigned to its constructs, as it supports mission operations. Understanding that the value reflects the asset's utility in supporting mission operations is essential to proper and correct value assignment. Value levels are assigned to contextual value constructs, with total contextual value being a function of a weighted average of the value constructs.

Value Level 5.

Value Level 5 reflects an asset or asset construct that provides critical support of a mission process. Loss or degradation of this asset or construct will directly result in a failure of the information process it supports. It is important to note at this point that the CDA-D/MIA methodology focuses on the identification, documentation, and valuation of *critical* information assets to determine impact to mission capability when such critical assets are compromised. It is important to understand at this point that the methodology is designed to be self-scoping to exclude all but those assets critical to mission operations. The CDA-D/MIA methodology for identification, documentation, and valuation of assets is discussed later.

Value Level 4.

Value Level 4 reflects the value of an asset or asset construct that provides an important contribution, but not critical support. Loss or degradation of the asset or construct assigned this value will greatly impede the information process it supports, but not singly cause process failure.

Value Levels 3 through 1.

The remaining value levels reflect a graduate reduction in the utility value of the asset for mission operations through the supporting information processes. Value Level 3 reflects the value of an asset or asset construct that provides some utility contribution, but would not result in significant impediment to mission supporting information processes if the asset or construct was compromised. Value Level 1 indicates the asset presents very little mission critical utility within the organization. This is not to say the asset is valueless in other ways. However, if the asset was compromised in some way, there would be little or no impact to the organization as a result of the asset's compromise.

Due to the self-scoping CDA-D/MIA methodology, it is not expected that a great number of the critical assets identified and ultimately valuated will be initially assessed a value less than Value Level 3. However, this is just an expectation of the researcher. The nature of the asset and its contextual value may produce wide deviation between the Value Levels assigned to individual constructs. It should also be noted that this expectation addresses pre-incident asset valuation only. A compromise may cause a high level of temporary asset devaluation caused by degradation in the asset's utility within the organization through some compromise of confidentiality, integrity, or availability. Such devaluation is damage, and will be discussed further below.

Estimation of Damage through Value Loss.

The goal of the CDA-D/MIA methodology is to assess mission capability impact through cyber damage assessment following a successful cyber attack. Value is assigned to all constructs of the asset value model to determine pre-incident value and value loss can occur from both internal and external factors. The scoped nature of damage, as previously discussed, implies that damage determination need primarily deal with those constructs which may be directly impacted by external factors introduced through an incident; specifically those sub-constructs, confidentiality, integrity, and availability which comprise the asset's state value construct.

This research defines *damage* is some function loss of value within the contextual value constructs caused by an incident. This loss of value is a direct reflection of the asset's utility caused by some external influence that affects the asset's confidentiality, integrity, availability, or any combination of these three. Generally, damage in information asset is not permanent and is only becomes so if the asset is compromised in such a way that it cannot regain its previous level of utility to the organization. Examples of permanent damage are a compromise of confidentiality that prevents the information from being used anymore; or a natural disaster where the information asset, its container, and all backups are destroyed and the asset cannot be restored.

Damage in the Domains of Operations.

The tactical, operational, and strategic domains of operations are defined and identified by their respective time constraints. Assessing damage across the various domains of operations requires assessing different constructs of the asset's state value to determine loss in terms relevant to the constraint of the specific domain. This section

will concisely discuss each and describe how critical asset damage occurs in the value constructs.

Damage in the Tactical Domain.

Information assets that reside exclusively in the *tactical* domain of operations generally have a relatively short life cycle. Often, the information assets used in the tactical domain are not stored in a static container, but exist as an information stream. Examples of tactical domain information assets include such important real time information on which decision makers depend, such as UAV feeds and other targeting feeds that provide the commander battlespace awareness in the here and now. These real-time assets have become critical to AOC operations and loss or damage would certainly affect the commander's mission. However, it should be noted that not all assets that *exist* in the tactical domain of operations reside exclusively in this domain. There exists many information assets with extended lifecycles that still present commanders with utility in tactical operations.

The difficulty in measuring damage to tactical assets is a product of the short lifecycle of the information asset. This domain of operations require that damage and mission impact assessment occur rapidly to provide the decision maker with assessment information for timely use in the time constraints of tactical operations. When an incident occurs, there may be insufficient time for an incident response team to work with the incident owner to assess fully the damage in terms of a value loss model. This holds especially true if the asset is an information stream, rather than a file accessed on a server.

These issues underscore the previously discussed importance in the difference between potential and actionable value. When an incident occurs in the tactical domain, the primary concern is the availability construct. In terms of actionable value and damage, this availability can directly be translated to the organization's ability to use the asset—can he get the information he needs right here and right now? If the answer is no, the actionable value is reduced and damage has occurred because of the incident. Incidents affecting the confidentiality and integrity constructs are not forgotten, but will generally not be assessable in the time constraints imposed by tactical operations. Since the CDA-D/MIA methodology advocates the pre-incident valuation of critical assets, it becomes possible to immediately know the potential mission impact resulting from the incurred damage. By estimating the potential mission impact through strategic determination of asset potential value, some degree of predictive damage and mission impact can be accomplished in the tactical domain; even without explicit technical support provided by an incident response agent.

This, however, is only a first step and meant to describe those CDA-D/MIA methodology actions that may occur in the time constraints of the tactical domain. Most incidents outlive the tactical time constraints and move into the operational domain. Determination of defensive cyber damage in the operational domain is discussed in greater depth in the following section.

Damage in the Operational Domain.

Damage and mission impact assessment in the *operational* domain is the area most suited for employment of the CDA-D/MIA framework, and the domain in which the greatest benefits are realized. In this domain, information asset life cycles span a time

great enough for the incident response to coordinate with the information owner to determine value loss. Since the asset's potential value is determined in pre-incident activities, the information owner can know immediately the potential damage and potential associated mission impact caused by the incident. It is important to understand that the information owner is responsible for assigning the degree of construct and asset devaluation based on the technical assessment analysis provided by the incident responder and the levels of criticality assigned in the initial asset valuation.

The constructs suitable for damage assessment in the operational domain are illustrated below (see Figure 14 below). These constructs allow the information owner to model the assessed damage affect on the usability of the information asset by reducing the actionable value in the constructs that were affected by the incident. This reduction in value reflects loss of asset utility in support of organizational goals, affecting the

actionable value but not the potential value of the asset.

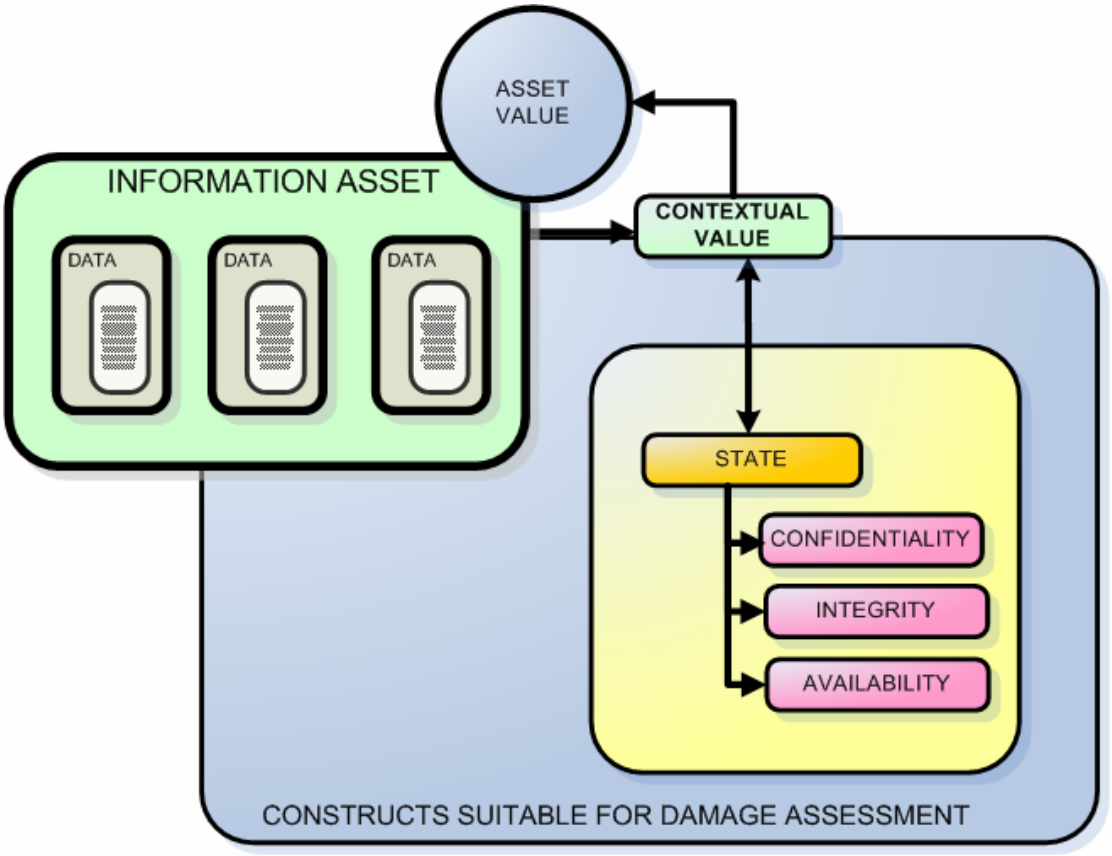


Figure 14. Asset Value Constructs Susceptible to Damage-induced Devaluation

Value Loss in the Strategic Domain.

Since damage is defined as value loss resulting from a successful cyber incident, value loss resulting from damage is generally restricted to the tactical and operational domains. Construct value loss can occur in the strategic domain however and must be reflected within the asset's value constructs to ensure effective and proper asset risk management and accurate values which facilitate accurate damage assessment when a cyber incident occurs. Construct value shift can occur as the result of changes within the organization, or simply through the passage of time. Some examples of this are changes

in the organization's mission which affect the asset's utility in supporting the new mission objectives. Likewise changes in infrastructure technology may result in the creation of a new information asset that makes the current asset obsolete. Both of these examples directly affect the asset's mission binding construct. Time is also a factor if the information asset *outlives* it relevancy to the organization. Since the information is less relevant, the asset's utility to the organization is diminished and the value of the asset's age factor must be made to reflect this shift.

The value of the identified critical information assets must be re-assessed at regular intervals to ensure that the previously assigned value is still meaningful and useful in damage assessment. This maintenance is as critical to successful damage and mission impact assessment as the initial asset identification and valuation.

Measuring Mission Impact as Mission Degradation.

The CDA-D/MIA methodology is founded on identification and valuation of information assets for the ultimate purpose of mission capability impact assessment following a cyber incident. The CDA-D/MIA methodology employs a top-down methodology for identification of these critical assets which identifies the dependency relationships between the critical information asset and the critical mission operational process or processes it supports. This inherent asset-to-mission mapping which results from this methodology is a central part of the CDA-D/MIA methodology. It is the catalyst that allows critical asset damage to be mapped to mission capability impact.

Establishment of an Impact Scale.

Impact assessment, like damage assessment is a qualitative estimation. For any mission impact metric to be useful, it must accomplish two critical tasks. First, it must

translate damage to the cyber information assets on which the organization depends into an accurate reflection of the impact to the organization's mission. Secondly, it must present this impact to the organization's decision maker in terms that allows the design making agent to make smart and correct decisions quickly and accurately.

This thesis has discussed loss as a qualitative estimation of reduction in actionable value of the critical information asset. Remember that assessing this loss it to estimate the degree to which the critical information asset's utility has been reduced; and that reduction in the critical asset's utility implies a potential reduction in mission capability. This reduction in mission utility is realized as mission impact in those processes that depend on the effected asset. As this value decreases, the theoretical impact increases. All things being equal, therefore, value and impact maintain an inversely proportional relationship. The decision maker operating in the tactical or operational domain cares little about these technical aspects of value reduction that about mission impact, however. The decision making must be presented with impact assessment metrics that immediately provide situational awareness regarding the impact to his/her organization's mission capability. To meet this need, this research proposes a scale similar to the Value Rating scale proposed earlier in this paper (see Figure 15 below).

Figure 15. A Five Point Scale for Mission Impact Assessment and Reporting

This proposed scale serves the purpose of providing a simple to understand estimation of the qualitative mission impact assessment. The scale is designed to provide a human decision-maker with a single-look situational awareness of the mission impact assessment at the time of reporting. The impact scale is meant to be a part of a graphical executive summary of the impact level. The Incident and Impact Report in which it is presented will contain further detail about the technical details and potential or actual mission impact specifics.

Ideal Implementation of the Impact Scale.

The impact scale will ideally be presented in a graphical user interface of an automated reporting system. Refined damage models will ideally translate damage assessment to mission impact will provide the commander with the incident and impact report rapidly, producing faster battlespace awareness of friendly mission capability. To be most effective the scale must be presented in a graphical format, with mission impact Y-axis shown over time on X-axis. This would allow the organization decision maker to visualize both potential and actual mission impact as more technical information about the incident becomes available over time. The following figure presents a conceptual graphical application of the value scale from initial potential mission impact assessment through graduated refinement though interim assessments. (see Figure 16 below).

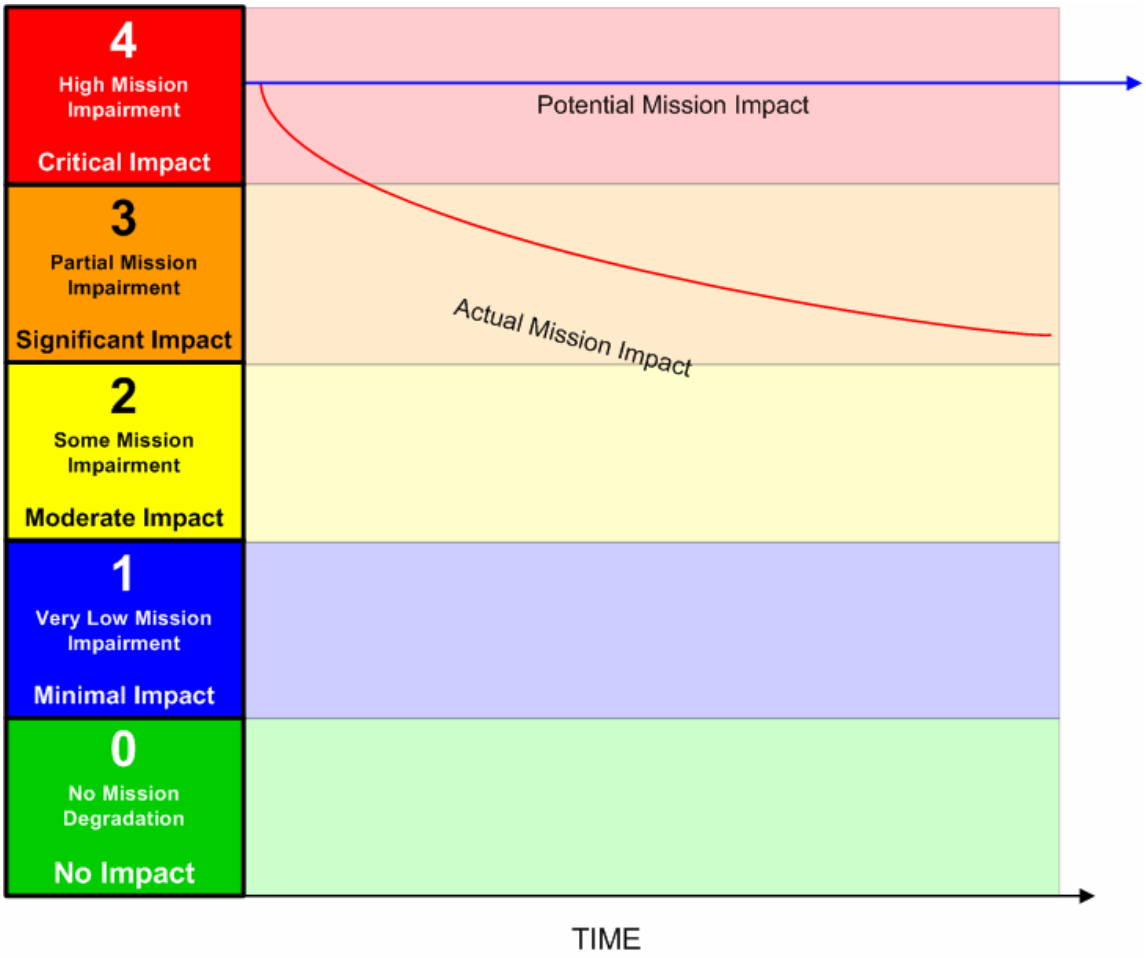


Figure 16. Conceptual Graphical Application of Value Impact Scale

Conceptual Methodology for Cyber Damage and Mission Impact Assessment

This section presents a conceptual methodological framework for establishing and implementing cyber damage and mission impact assessment. Cyber damage and mission impact assessment is not a single task. Instead, it is a system of activities that rely upon each subsequent activity to correctly implement its responsibilities correctly to facilitate the ultimate goal of providing the operational decision maker with improved situational awareness through accurate and efficient mission impact reporting. As this research has shown in the state of Air Force and DoD damage and mission impact assessment

activities, a failure in any of the subsystem activities results in a failure in mission impact assessment capability.

Overview of the CDA-D/MIA Methodology.

The CDA-D/MIA framework is comprised of three main stages: pre-incident activities, damage and mission impact assessment, and reporting. The foundation of defensive cyber damage and mission impact assessment is pre-incident asset identification, valuation, and documentation. For accurate defensive damage assessment to occur, the organization must have developed a portfolio of profiles of its *critical* information assets before the incident occurs. When the incident occurs, the asset owner and the incident responder must work together in their respective roles to determine what information assets were affected by the incident and what damage was incurred. The incident responder is responsible for producing a technical assessment of the incident to allow the information owner to understand which assets were affected by the incident. The information owner may then use the asset profiles of the affected assets to determine the damage. Assuming the asset was correctly documented, the owner may then quickly determine the impact to mission capability. This impact assessment may then consolidated and reported through existing reporting channels to provide fast notification and reaction to the incident.

The CDA-D/MIA methodology is founded on the identification, valuation, and damage assessment of *critical* information assets. Modern organizations and especially military operations depend on vast amounts of digital data and information stores to operate. Attempting to identify and document all information assets within an organization would quickly prove an overwhelmingly vast and insurmountable objective.

The loss of certain information assets would cause great harm to the organization's mission capability; the loss of others may hardly be noticed. Critical information assets are those information assets which directly support the organization's mission. Therefore the CDA-D/MIA methodology's seeks to identify, document and valuate those critical assets owned by the organization to allow accurate and effective defensive cyber damage and mission impact assessment when an incident occurs..

CDA-D/MIA Application Across Domains of Operations.

The military recognizes three primary domains in which operations occur: tactical, operational, and strategic. The CDA-D/MIA methodology can provide the decision maker situational awareness in each of these domains. However, as the time constraints existing within each operational domain grow smaller, constraints are introduced in the CDA-D/MIA methodology's application. The CDA-D/MIA methodology requires certain activities to occur in certain operational domains more often, and restricts activities form occurring in others. The following figure provides a conceptual illustration of how the CDA-D/MIA activities on an incident timeline approximately map through the domains of operations (see Figure 17 below). This figure is only a notional example, but provides a good example of how activities would align with the CDA-D/MIA activities.

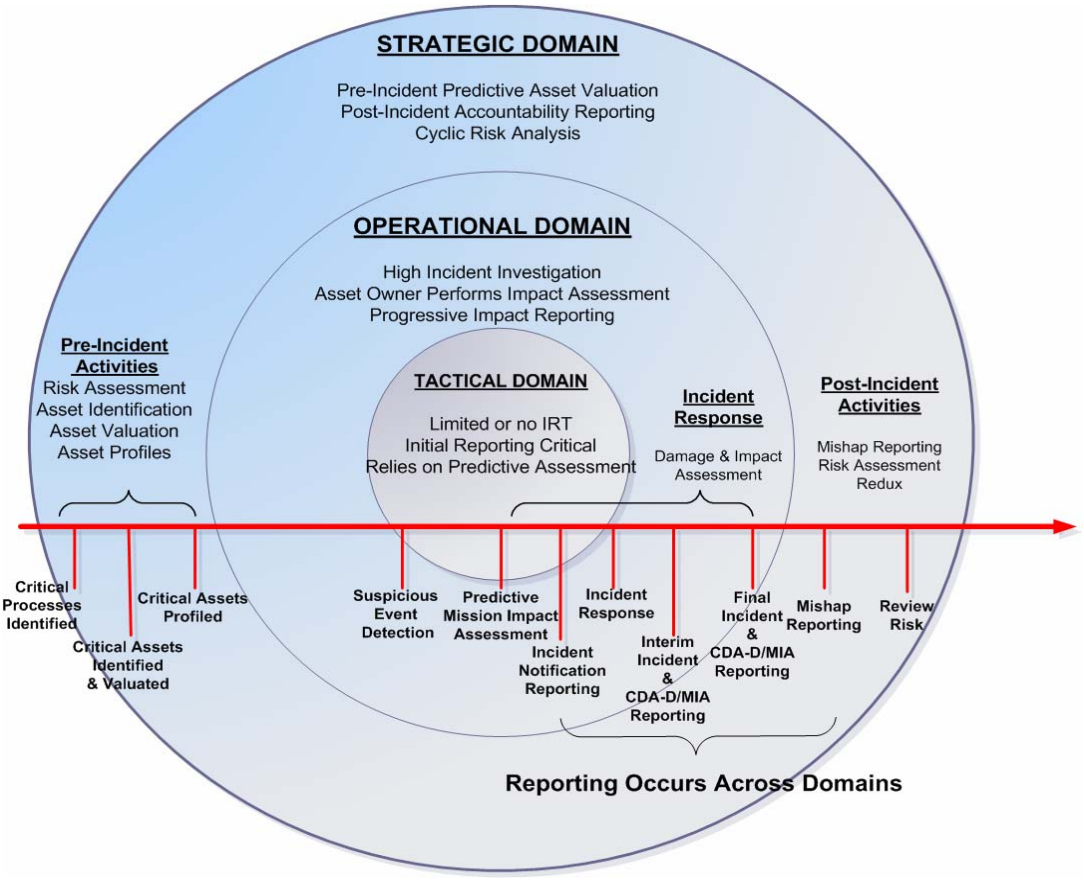


Figure 17. Key Mission Impact Activities Across Domains of Operations

For example, risk assessment that facilitates critical asset identification and valuation must occur prior to the incident to allow effective damage and mission impact assessment. These pre-incident activities occur in the strategic domain. The tight time constraints of the tactical domain often preclude all but the basic response activities since the tactical commander cannot wait until incident investigation to understand how/her mission has been impacted.

Pre-incident Activities in the Strategic Domain.

All assumptions of the CDA-D/MIA methodology are based on accurate identification, documentation and valuation of the organization's information assets

before an incident occurs. Therefore, the preparatory activities an organization takes before an incident occurs are essential to the successful cyber damage and mission impact assessment (see Figure 18 below). The pre-incident activities of CDA-D/MIA methodology that allow the required *front loading* of the damage assessment framework are accomplished in four essential phases. Each of these comprises a step in the top-to-bottom identification of the critical assets that enable the organization to accomplish its mission. A validated and asset-focused risk management framework such as OCTAVE can effectively assist the information owner to identify and document information assets that are valuable to the organization and focus risk analysis activities on the critical assets identified (Alberts, Dorofee et Al. 2003, pp. 3-5). The asset identification methodology advocated by this research is a top-down, operations-oriented, and asset-focused approach. A high-level view of critical pre-incident steps are as follows:

- Define the organizational mission
- Identify, define, prioritize, and document the operational processes that support the mission
- Identify, define, enumerate, prioritize, and documents the information processes that support operational processes
- Identify, define, document, and valuate the information assets that the information processes depend upon.

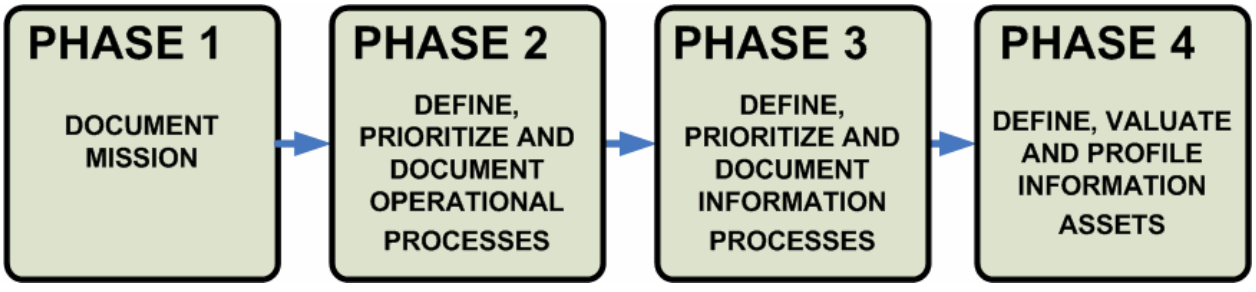


Figure 18. Asset Identification and Documentation Process

Critical Information Asset Identification.

Before valuation of critical information assets within an organization can be accomplished, they must be identified. To do so, employing an effective information asset-focused risk assessment methodology is essential. The approach to risk determination is very important, and this research proposes a departure from risk assessment methodologies that focus on technological assets.

Risk exists where threat to an asset and a vulnerability in the asset intersect. However, identification of the wrong asset negates the benefits of risk analysis. This research proposes that risk to cyber information assets exists explicitly as risk to the information assets that exist within the technological infrastructure and vulnerabilities are shortcoming in the security controls designed to protect these information assets from malicious or non-malicious incidents (see Figure 19 below).

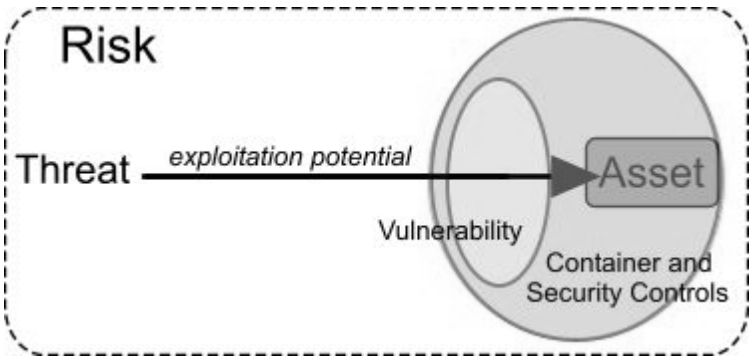


Figure 19. Risk To the Asset Within the Container

There are several proven asset-focused risk assessment methodologies from which to choose, including Carnegie Mellon University's OCTAVE methodology. It is

imperative however that the methodology selected facilitate a top-down, operations oriented approach to identifying the critical information assets on which the organization depends.

Critical information assets exist within every organization with information dependencies. These assets are the at the core of modern military operations. The dependencies upon information exist in dependency layers of organizational processes, as show in the following figure (see Figure 20 below). Accomplishing the organizational mission depends on individual and integrated mission operational processes. Many of these operational processes depend upon information flows, or information processes. These information processes rely upon one ore more information assets. A failure of a critical information asset could generate an upward ripple effect that impairs one ore more critical information flows, which cripples a mission process with the ultimate effect of impairing the organization's mission. By following this internal chain of dependencies the information owner can identify the organization's critical information assets by drilling-down from the top, starting with identification of the organization's mission, and ending at the bottom with the information assets on which the organization depends.

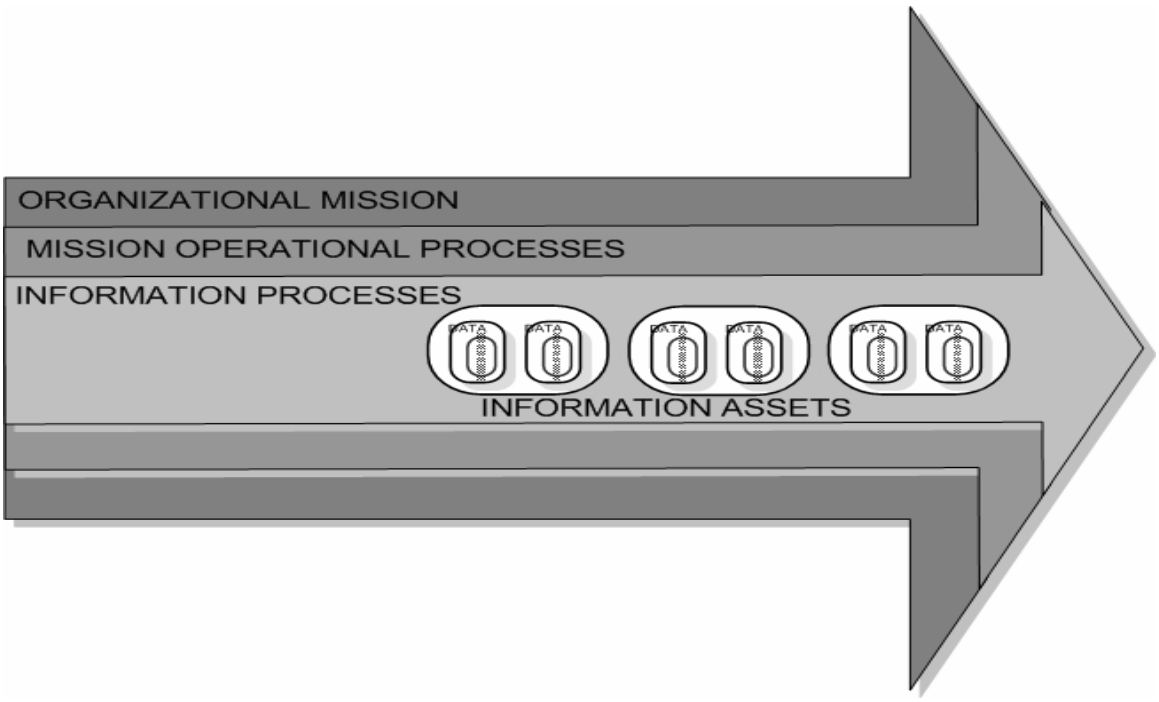


Figure 20. Information Assets as the Core of the Mission Operations

Establishing Relative Ownership

As the head of the military organization, the commander is the information owner. The information owner bears the responsibility for identification of critical information assets, which is an important but difficult task at the onset. For this reason, the commander will necessarily delegate ownership to an a responsible organization member to act on his/her behalf to execute asset ownership duties and responsibilities. However, the commander *must be diligent* when delegating this responsibility. Accurately establishing information ownership is essential to successful CDA-D/MIA efforts. The delegate information owner must possess both a clear understanding of the organizational mission and the appropriate operational perspective to identify the critical processes within the organization that directly support the mission. When acting on behalf of the commander, the delegate effectively becomes the information owner.

Identification of Critical Mission Processes.

Accurate and comprehensive mission impact assessment through cyber damage assessment depends explicitly on identification of those critical cyber information assets without which the mission would be impaired or fail. Therefore, the CDA-D/MIA methodology strongly advocates the identification of these critical assets by starting with the mission they support. This is the reason why the information owner must possess the appropriate level of operational perspective when beginning to identify the critical assets in the organization.

First, the information owner must clearly define the organization's mission, to include the upstream missions it supports, and the downstream mission that support its mission. This is important, as it aids in identifying other organizations whose mission may be affected by a mission-impacting cyber incident. When the mission and any important high-level mission dependencies are identified, the information owner must next identify, *rack and stack*, and document the mission's operational processes which enable the organization's mission to exist. The information owner must identify, enumerate, and prioritize each process, defining how the each operational process supports the organization's mission.

It is important to understand that prioritization of operational processes is to facilitate identification of the organization's *critical* processes. Prioritization and assigning criticality values to each identified operational process facilitates the self-scoping process to exclude those processes that are less important to the organization's mission operations. This basic establishment of criticality is the first step in identification and valuation of the critical information assets that will be ultimately identified. The

CDA-D/MIA five-point value scale should be used to *rack and stack* each process. A *Value Level 5* is assigned to those processes assessed as critical to mission support.

Each critical process must be documented to ensure record of its mission support, mission criticality rating, and other important information is maintained. It is important to ensure accurate documentation for further identification of supporting processes, and ultimately facilitation of damage to mission operations impact mapping after an incident. This documentation will be maintained in the associated information asset profile discussed later.

Identification of Critical Information Processes.

The next phase is the identification and documentation of critical information processes. In this phase, each operational process identified as critical to the organization's mission must be examined to identify the *information processes* that support that operational process. As with mission processes, these information processes must be enumerated and prioritized by criticality using the same five point value scale to annotate the information process' criticality to the critical operational process it supports. Also like the previous phase, the critical information processes that support critical operational processes must be documented in the same way as the previous phase.

Identification of Critical Information Assets.

The process thus far has been a self-scoping process to identify the organization's most valuable cyber information assets in terms of mission enablement. Beginning with the mission, organization's most critical operational process are identified; allowing the most critical information processes supporting these critical processes to be identified. The stage is now set to identify the information assets that directly support these critical

information processes. Identification of the critical information assets within the organization is the most important activity of the CDA-D/MIA methodology.

Once critical information processes have been identified, the information owner must determine what digital information supports these processes. As in the previous stages, the information must be identified, documented and assigned a value. Critical information assets are the epicenter of the CDA-D/MIA methodology, so it is important to understand how value is assigned. As previously discussed, the value of the information asset is derived by its utility for the organization to meet its mission goals. Since the identification methodology has led the information owner to the information assets supporting the organization's most important information processes, which in turn support its most critical mission operational processes, the assets identified are all very important to the organization's mission capability. However, not every asset is equally critical since damage to one asset may result in a lesser degree of degradation to the information process that it supports.

Identification of Critical Asset Containers.

It is important that the infrastructure asset on which the information resides be clearly identified and documented. Identification of the information asset container is essential for generating mission to supporting system mapping. In relatively stove-piped systems, this support may be self evident, but in many mission processes that depend upon information assets shared over a network, the physical location of the information asset may not be as readily known. Knowing which system contains the asset is especially important during incident response. Incident responders, by necessity, will perform response activities to assess damage to the technological infrastructure resulting

from a cyber incident. Container documentation in the information asset profile will facilitate a more rapid understanding of potential mission impact by bridging the gap between the system and the information asset, which will lead to more efficient assessment of mission capability impact.

Critical Process Documentation.

All aspects of an organization's information assets must be well documented to be an effective tool for damage assessment. This includes documentation of the critical mission operational and information processes that the organization relies upon. Documentation of these processes is critical to the success of damage and impact assessment since such documentation provides mapping from the asset to the mission.

Documenting Critical Mission Processes.

Accurate and effective mission process documentation must be accomplished first. The information owner should use the proposed worksheet (see Figure 25, Appendix B) to ensure all important information is captured. By this time the information owner will hold an understanding of the processes critical to the organization's mission. Specifically, the mission process should be provided a unique mission process identifier (MPID) prevent any confusion between mission processes. It is also important that the agent responsible for the mission process is documents, to include contact information. This agent may prove valuable in the identification and valuation process, as well as damage and mission impact assessment following an incident. Any known impact to the mission must be documented, as this is an important factor in understanding the process' criticality to the mission. This worksheet must be

maintained to assist in the drill-down process to identify the organization's critical information assets.

Documenting the Critical Information Processes.

Documentation of the critical information processes is similar to the documentation of mission processes. The goal is to identify the information processes providing critical support to the organization's mission processes and to discover and document the information assets on which the organization's mission ultimately depends. The information owner should utilize the proposed worksheet (see Figure 26, Appendix B) to identify the important information about the critical information processes. It is important that the information process be enumerated and given an information process identifier (IPID) to uniquely identify and distinguish the information process. As with the mission process, establishing processes ownership is very important. The attached worksheet should be used to assist in documenting information processes within the organization.

Critical Information Asset Profile Documentation.

Documentation of the critical information assets is the foundation of damage and mission impact assessment. It is important that the information owner capture the appropriate information about both the information asset *and* the system on which the asset resides. As with process documentation, a set of worksheets is proposed to aid the information owner in this task. Asset and container documentation form the core of the Critical Information Asset Profile (CIAP). The CIAP contains all documentation used in identifying and valuating the asset; to include documentation of the processes that it supports.

Documenting the Critical Information Assets.

All key aspects of the critical information asset must be documented. At minimum, the following information is essential to documenting information in a manner which facilitates the capability to perform damage and mission impact assessment following an incident:

- Information owner and custodian, with contact information
- Information producer and consumers, if known
- Supported mission critical process(es)
- Criticality rating (value)
- A description of how the information asset is used
- The asset's container
- Additional important information

The proposed worksheets (see Figures 27 and 28, Appendix B) should be used to assist the information owner in this task of collecting the basic, but essential information about the asset. It is during the identification and documentation phase that the information owner must determine and document the value of the asset to the organization. The worksheet also assists the information owner in determining the value for the asset through criticality rating values assigned to its value constructs.

Documenting the Critical Asset Containers.

Thorough documentation of the critical asset containers is also extremely important. The container is the system on which the asset is physically located. Incidents that impact the container will likely impact the information asset. Documenting the relationship between the container and the information asset is important to the

information owner attempting to determine mission impact from the technical assessment information provided by the incident response agent. It is important that the information owner document such important information as the ID and location of the container, the contact information about the custodian responsible for the maintenance of the container, important technical details about the container, and any other information that may help map technical information to the information asset. The proposed worksheets (see Figures 29 and 30, Appendix B) will help the information owner document the important information about the container.

Information Asset Valuation.

Valuation of the asset is a qualitative estimation of the utility of the asset within the organization. The assumption is at the stage that the assets identified are critical to the organization. Not all recognized value constructs may have the same criticality to the mission, so the criticality of each must be considered independently. Unless there is information to indicate otherwise, it is assumed that no external factors are present to influence the value of any constructs at the time of valuation. The value assigned to each construct must reflect the criticality of that construct in its relative support for the mission. The proposed worksheet will assist the information owner in appropriately assigning value to each value construct.

Mission Binding Valuation.

The mission binding construct reflects the criticality of the asset to the organization's mission. Assets critical to critical information processes, which support critical mission processes will inherently be critical. This construct is relatively constant in the operational and tactical domains of operations.

Age Valuation.

The age value of an asset is a reflection how quickly it loses relevance in the organization. Most assets do not age beyond operational relevance excessively fast, however there are some such as weather reports that do. Age is not considered in operational and tactical damage assessment, because it is a temporal function generally unaffected by a cyber incident. But if the asset's age decay could cause impact to the mission, the information owner should value this construct at a rating that reflects this criticality. Those assets that do age rapidly should be annotated as requiring a periodic refreshment, with the defined refresh period also annotated. For example, a weather report may be provided hourly, with each successive report superseding the previous. The information owner must annotate this on the construct value worksheet that the asset is refreshed every hour.

Confidentiality Valuation.

If a compromise of this asset's confidentiality would have an impact on the mission, the information owner must value this construct accordingly. Also, it is important for the information owner to annotate on the worksheet how the mission would be impacted to the best of his/her understanding.

Integrity Valuation.

If a change in the data may cause impact to the mission the asset supports, the information owner must value the construct accordingly. The information owner must not consider the potential for back up and recovery when valuating the asset, but must assign the value as to the impact to the mission before any remediation or recovery actions can be undertaken.

Availability Valuation.

The information owner must assign a value to the importance of the availability of this asset to the mission. The owner must annotate the mission impact to the best of his/her understanding should the asset be lost. In many cases, short term loss of an information asset may not have great mission impact; with these affects being realized over time. At the time of valuation the information owner must valuate the asset with not assumptions of restoration. This will aid in determining the potential impact when an incident occurs.

Asset Profile Maintenance.

There are several concerns about the maintenance of information asset profiles. Once completed, these CIAPs will contain a large amount of information about the critical assets for the organization. All of an organization's CIAPs will be compiled into the organization's Critical Cyber Asset Portfolio (C-CAP). The C-CAP is simply the collection of all critical processes and cyber assets on which the organization depends. This introduces a new avenue of risk to the organization, as unauthorized access to the organization's C-CAP would provide a malicious actor a roadmap for targeting and attacking the critical assets that could cripple the organization's mission. For this reason, the organization's C-CAP must be maintained in some location safe from unauthorized access, but where the information owner has ready and immediate to the C-CAP access in the event of a successful cyber incident, to include catastrophic network failure.

Security issues aside, the issue of the sensitivity of the information about contained in the C-CAP the organization gives rise to a second issue that is equally important to the effectiveness of mission capability the CDA-D/MIA. This issue is

whether the C-CAP is maintained locally, or by a centralized agency, such as the AFNOC NCD with its responsibility for maintaining continual network operations and security.

Local C-CAP Maintenance.

When a cyber incident occurs, the information owner needs access to the information within the C-CAP immediately. In many cases, this may allow the decision maker to know the immediate potential mission capability impact, assuming that the critical information asset profiles are current and accurate estimations of the asset's state and value. Local storage would ensure expedited access to this valuable tool, allowing the commander to have almost immediate situational awareness of the threat to the mission. The downside is that by keeping the information local, notification of the damage an asset on which other agencies depend may be delayed. Having an agency with enterprise NETOPS authority and responsibility maintain all C-CAPs for the organizations in the enterprise may allow more rapid downstream incident damage and mission impact assessment.

Centralized C-CAP Maintenance.

While centralized management and maintenance of C-CAPs for all organizations in the enterprise may expedite damage and mission capability impact assessment, it re-introduces the problem of risk. As previously mentioned, the C-CAP could potentially provide a malicious actor a goldmine of information about where to attack the network to optimize mission impacting effects. If all the C-CAPs of all organizations within the enterprise are located in centralized storage and the security controls are defeated, the malicious actor would have not just a target map for one organization, but for the entire

enterprise. Aside from security risks, there may be political complications associated with releasing sensitive information of the organization to another.

For these reasons, the research proposes localized maintenance of an organization's critical information asset portfolios.

Automation of Profile Maintenance.

Whether stored locally or centrally, the organization's C-CAP must be automated. The proposed worksheets allow the information owner to collect the information needed to load a relational database for more rapid access to the organization's C-CAP for faster determination of mission impact. A notional ERD based on the data collected from the worksheets (see Figure 21 below) demonstrates how such a database would automatically link critical dependencies within the organization. This ERD is intentionally very high level and elementary, but it is easy to see how automation can allow a better understanding of information asset dependencies within the organization. Ideally, such database deployed across the enterprise, would lay the foundation for nearly instantaneous mission impact assessment, both predictive and actual.

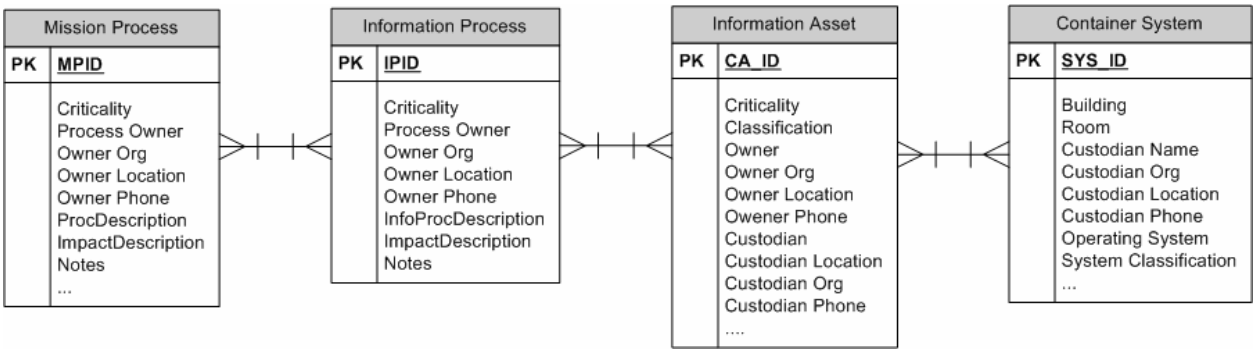


Figure 21. Notional Entity Relationship Diagram for C-CAP Automation

Incident Damage and Mission Impact Assessment Activities.

In the CDA-D/MIA framework, there is no noticeable change to the function and activities of incident response, as currently implemented in the Air Force. IR function will remain focused on the traditional activities of response, remediation, and forensic investigation. However, rather than being tasked with determining the impact of an information incident to an organization's mission, the IR function will work closely with the information owner, providing the technical details to allow the information owner to perform damage assessment at the site of the incident. The constructs of an asset-focused pre-incident valuation will allow the IRT and information owner to determine asset devaluation resulting from not only asset availability but also confidentiality and/or integrity compromise—an aspect not attainable under the current, infrastructure-focused assessment implementation.

This section will discuss the roles and responsibilities of those agencies involved with incident response, damage and mission impact assessment, and initial reporting and the conceptual implementation of these tasks.

Responsibilities for Damage and Mission Impact Assessment.

There are two aspects to performing defensive damage assessment: technical assessment and asset damage assessment. Technical damage assessment is the evaluation of damage to the organization's cyber infrastructure. It reveals such important evidence as how the attack occurred and what, how long, and by whom information assets were accessed, attack vectors in malicious cases, or the number of passwords compromised. Technical assessment must be accomplished to enable accurate asset damage assessment, but cannot tell the information owner the degree of value loss in the affected asset. The

technical assessment allows the information owner to determine this through asset damage assessment, which allows damage to be mapped to mission impact. This section will discuss the responsibilities for each of these important activities.

Technical Damage Assessment.

The technical damage assessment is critical to establishing what information assets were affected during a cyber incident. The technical assessment is a direct carry over of the damage assessment practices currently implemented on Air Force networks. It was previously stated that these assessments do not produce results usable for operational or tactical decision making. This statement is true, because technical assessment evaluates the very important aspect of impact to the infrastructure; but it cannot evaluate the impact to the information asset. Therefore, technical assessment is only the critical first piece of damage and mission impact assessment.

AFNOC NSD's Incident Response Team (IRT) is responsible for technical assessment of incidents on Air Force networks. The Air Force's IRT is a group of highly trained experts in cyber incident response activities. The IRT works through the AFNOC NSD with AFNOC NCD to coordinate and control all incident response activities on Air Force networks. The IRT is tasked to be the technical lead on these activities and is responsible for the post-incident response, handling and *technical* damage assessment of cyber incidents. As the technical lead, the IRT is also responsible for coordinating centralized incident reporting throughout incident life cycle.

Because the CDA-D/MIA methodology operates across all operational domains, there are some cases in which the time constraints of the tactical domain may preclude traditional IRT technical assessment. In such situations, the mission cannot allow the

affected system to impair the mission long enough for traditional IRT response and technical assessment. In this case, another agent must act as an *incident response*(IR) agent to perform *stop-gap* technical assessment to provide the information owner information about the systems affected by the event or incident, and conduct immediate response and remediation efforts to ensure mission continuity. For example, in some tactical situations, time constraints may require that the extent of technical assessment be the server room technician providing the information owner limited details on which servers have failed. For this reason, the agent responsible for providing technical damage assessment is called the IR agent.

Under the CDA-D/MIA methodology, the IR agent would continue to perform its assessment and provide the result to the information owner at the site of the incident. As mentioned, the IR agent is already performing excellent technical assessment following cyber incidents. The IR agent also currently works directly with the local information owner in an attempt to better determine impact. Therefore, the implementation of a CDA-D/MIA methodology for damage assessment would add no new tasks to the IR agent's current responsibilities. Rather the CDA-D/MIA delineates the roles of both the IR agent and the information owner in determining damage following a cyber security incident.

Asset Damage Assessment.

The information owner bears the responsibility for both asset valuation and asset damage assessment. The information owner is the only entity with the perspective to determine the value of an information asset to the organization. The information owner will work with the IR agent to understand the technical assessment and how best to apply

the technical assessment to determine the extent of damage to the information assets. The information owner will assign a damage assessment based on the reduction in the assets utility resulting from the incident. This damage assessment will be used to perform the mission impact assessment that will be reported.

Mission Impact Assessment.

The mission impact assessment is the most important aspect of the CDA-D/MIA methodology. This assessment must be accomplished by an agency with appropriate perspective of how the damage will affect mission capability. Only the information owner can make such a determination. The information owner is responsible for using documented mission criticality and asset attribute information in the C-CAP to determine what missions may be affected by the damage incurred in the information asset.

Mission impact assessment will initially be predictive, based on the potential mission impact expected during the initial information valuation in the pre-incident risk assessment activity. However, as the IR agent continues to work with the information owner, providing more refined interim technical assessment, the actual mission impact may be realized as less than initial expected. The information owner is responsible for reporting this refined mission impact assessment in each interim incident report. Although the information owner is responsible for mission impact assessment, it must work closely with the IR agent to ensure updated and accurate interim reporting.

Responsibilities for Assessment Reporting.

Incident and impact reporting (IIR) is as important as the assessment itself. Current reporting contains only technical assessment information. The IIR mechanism extends existing reporting content to contain the necessary impact assessment provided

by the information owner. The report must convey the nature and impact of the cyber incident as quickly as possible to the decision maker in a way that may be easily assimilated into the decision making process. Both the IRT and the information are responsible for working together to compile and release an accurate report in a timely manner. There are three basic reports to be presented to the decision maker: initial report, interim report, and final report. The initial report is the initial notification of the incident. This report must declare the nature and classification of the incident and known technical information to facilitate rapid response action. However, under the CDA-D/MIA methodology, the initial report will also contain potential mission impact to advise the decision makers and NETOPS community of potential mission impact, thus provide an additional degree of battlespace awareness that currently does not exist. It is the responsibility of IR agent and the information owner to compile this information quickly. The potential mission impact is based on the assumption that the information assets' value and mission relationships were correctly assessed and documented in the C-CAP. The initial report will be followed by any number of interim IIRs which provide updated information on the status of the incident investigation, remediation and recovery efforts, and refined mission impact. Again, the information owner must work closely with the IR agent to develop the most accurate mission impact assessment. The final IIR provides the decision maker with notification of incident closure.

Conceptual Damage and Mission Impact Assessment Implementation.

This section describes in further detail how damage and mission impact are conceptually conducted in the CDA-D/MIA methodology. It is important to remember that the CDA-D/MIA methodology is intended to assess damage and mission impact in

the organization where the incident occurred and provide rapid reporting of the assessment results to both the local decision maker, NETOPS command and control structure, and the appropriate interested report consumers.

Incident Declaration and Predictive Mission Impact Assessment.

Damage assessment is an inherently post-incident activity. Under the current damage assessment methodology the commander is can gain neither a timely nor accurate understanding of the potential mission impact resulting from an actual or *suspected* cyber incident. The CDA-D/MIA methodology, as applied in the tactical domain of operations (see Figure 22 below), offers the decision maker predictive mission impact assessment in that time period between detection of a suspicious network event by the network defender (T_e) and the declaration of cyber incident by the incident response agency. The information owner cannot act upon a suspicious event until notified. Once the information owner is notified of suspicious activity on a system or systems identified to contain information assets (T_0), the decision maker is provided awareness of the potential impact to the mission. While investigation into the event is concurrently conducted, the information owner makes a predictive mission impact assessment based on the predictive valuation of the information assets potentially impacted by the suspicious event. The network defenders will only be able to provide technical information to identify what systems may be involved in the suspicious activity. Assuming the asset container was correctly assigned to the information asset and documented in CIAP and stored in the C-CAP, mapping the system to the critical asset is elementary. The information owner can determine if the system is a critical container, determine which critical assets are threatened, and determine a potential mission impact. At this point, mission impact is

predictive and will be equal to the maximum impact assigned during pre-incident valuation (T_1). The decision maker will now be able to make decisions based on this potential mission impact (T_2), allowing greater situational awareness in decision making in this interim period until more granular damage and mission impact assessment may be conducted. This tentative mission impact assessment is kept locally until such time the event investigation reveals incident threshold is meet and an incident declared by the IR agent activity. At this time, the predictive mission impact assessment is included in the initial Incident and Impact Report (IIR) provided to the Netops community through the existing consolidated reporting structure (T_3).

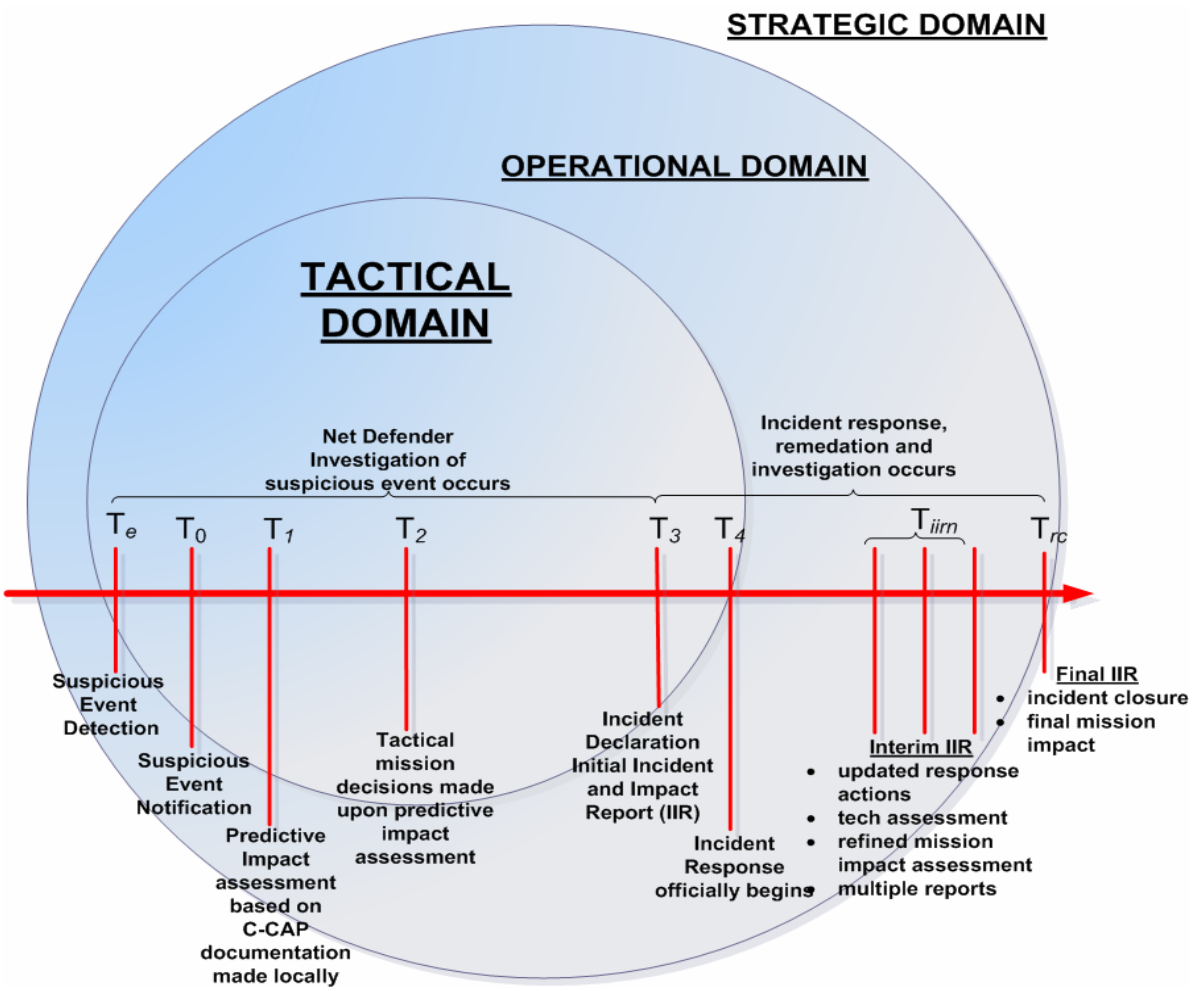


Figure 22. Mission Impact Assessment in the Tactical and Operational Domains

Incident Response and Damage Assessment.

Incident response officially begins with the declaration of an incident. Incident response, therefore, is inherently post-incident. Incident response, particularly the technical assessment, must occur for actual damage and mission impact to be assessed. This does not imply that IR agent personnel have no role in event investigation. In fact, the IR agent must be involved to ensure the event meets the threshold of escalation to incident declaration. However, IR agent activities cannot begin until post-incident;

specifically including technical damage assessment. This is especially true in incidents caused by non-malicious events.

With incident declaration, the IR agent will coordinate with the information owner to help establish initial damage and mission impact resulting from the incident (see Figure 23 below). The technical impact assessment will be provided to the information owner by the IR agent. The information owner uses the technical assessment to understand which information asset containers may be affected by the incident in the initial technical assessment, and the degree of exposure that may have occurred based on interim technical assessments. Based on these technical assessments the information owner can begin to estimate damage by comparing the amount of critical information asset exposure to the threat. The information owner and the IR agent work together to determine if the threat has been actualized and resulted in any damage to the asset.

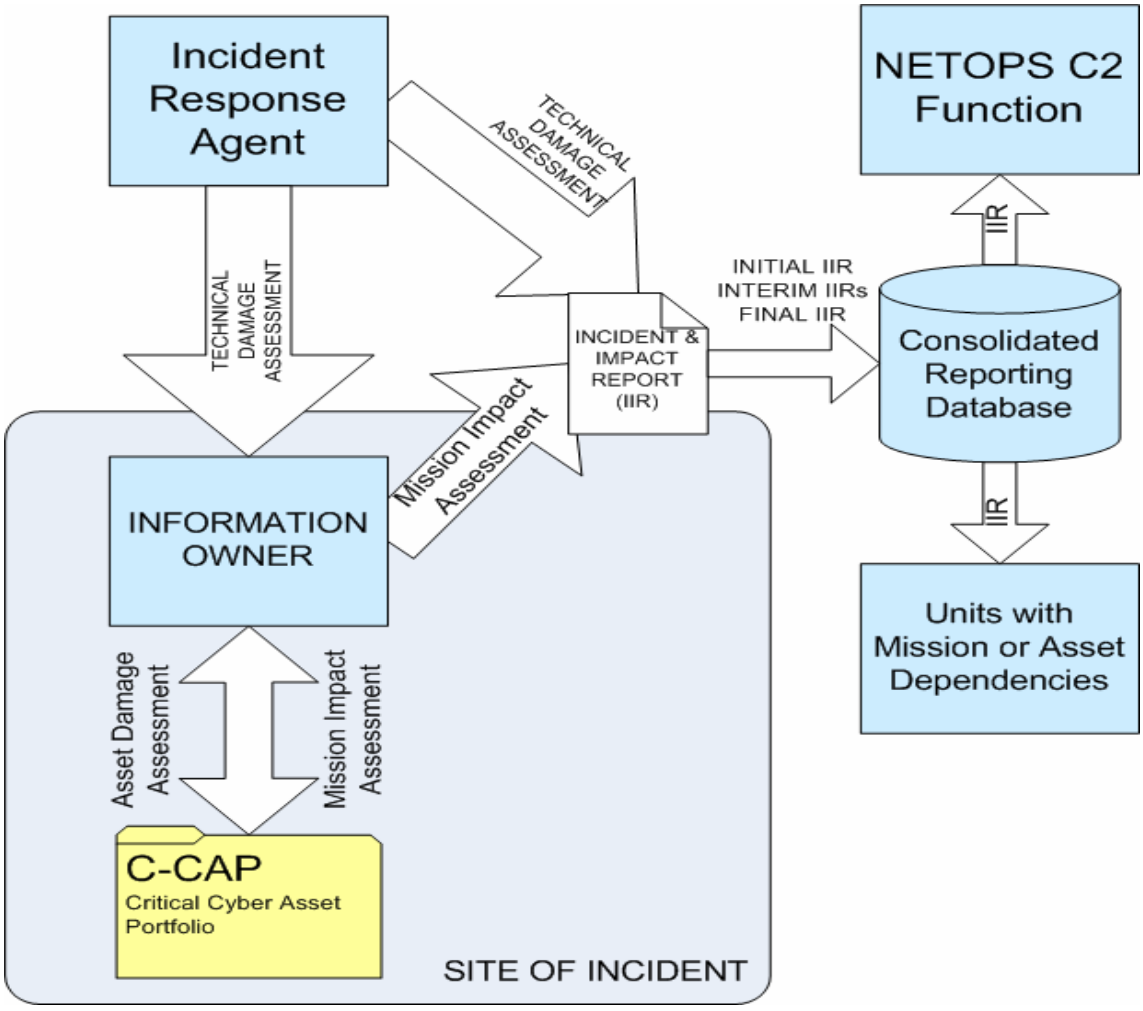


Figure 23. Notional CDA-D/MIA/MIA Incident and Impact Reporting

As previously discussed, damage to the asset is reflected in terms of reduction in utility; therefore if any reduction in the asset's usability to the organization results from the incident, the assets value is potentially reduced and reflected as damage to the asset. The amount of damage is based on the original valuation performed in the strategic pre-incident phase and recorded in the CIAP, stored in the organization's C-CAP. Any damage reflects a reduction of the actionable value of the information asset. The potential value as documented in the asset's CIAP, however, remains constant for the duration of the incident.

Value is reflected and shifted using the established five-point value scale. The information owner must consider the individual constructs of the value model when determining damage. If the technical assessment indicates a compromise of confidentiality, the information owner must consider what extent this construct was damaged and adjust the construct value accordingly to accurately reflect the resulting immediate utility of the asset. Damage can only be accurately assessed by the information owner by working with the IR agent to determine the type and extent of exposure the asset experienced. In this sense, damage may be as contextual as information valuation.

As more technical information about the incident becomes available to the information owner through interaction with the IR agent, this damage assessment can be reflect less damage than initially thought. Before any critical information asset damage assessment becomes truly useful, however, it must be mapped to mission impact.

Mission Impact Assessment.

Damage assessment cannot provide the organization's decision maker actionable information on which to make mission decisions following a cyber incident. Therefore, the information owner must be able to understand how the incident impacts the organization's ability to accomplish mission objectives following an incident. Determining asset damage must be accomplished to allow the information owner to determine the impact to the mission.

Mission impact assessment is a function of the damage assessment process. Therefore mission impact assessment may be revised over time and as more information about the incident becomes available (see Figure 24 below). The goal of mission impact

assessment is to provide the organizational decision maker with situational awareness about actual mission impact resulting form a cyber incident. However, actual mission impact may not be fully determined until the full extent of technical damage is known.

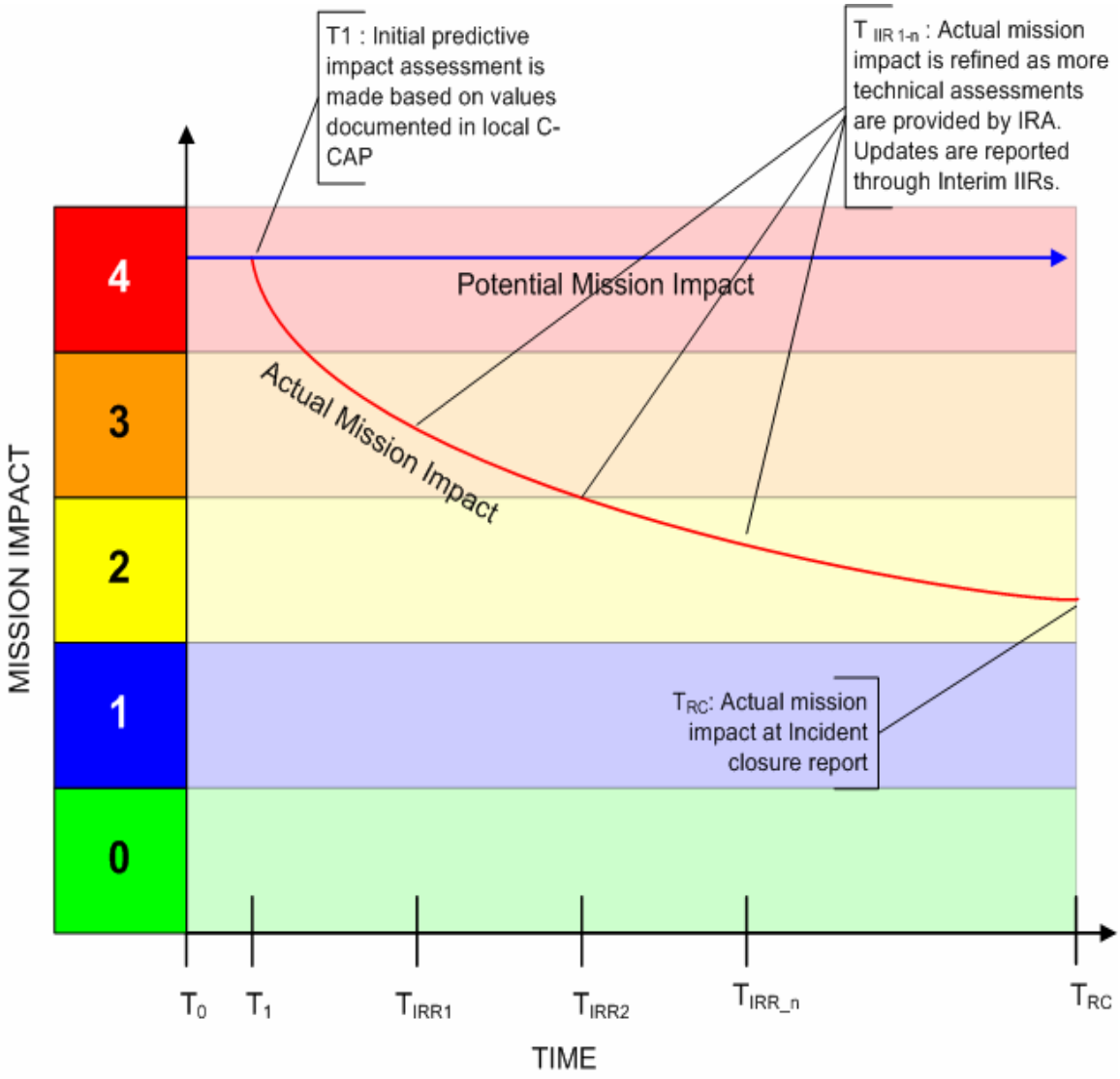


Figure 24. Graduated Refinement of Mission Impact Reporting Over Time

Mission impact assessment cannot begin until after the information owner is notified of either suspicious activity on the network, or that an incident has occurred (T_0).

After notification, the information owner can immediately perform an initial mission impact assessment (T_1). Because only basic information is known about the event or incident, the information owner must assume the actual impact to be equal to the potential impact established during strategic pre-incident asset documentation. However, as time progresses and more technical information is made available through coordination with the IR AGENT, the mission impact may be revised and show that actual impact is less than originally estimated. This revised actual mission impact assessment is provided included in interim IIR updates ($T_{IIR1...IIR\_n}$) which continue indefinitely until the incident is closed and the final IIR report of closure (T_{RC}) is submitted. Mission impact is assigned by the information owner using the five-point impact scale previously established in this paper.

Incident and Impact Reporting.

The IIR is the vehicle in which situational awareness relating to cyber information is provided to the organizational decision maker. The IIR presents both technical information pertaining to the incident and the resulting mission impact. IIR reporting also serves the purpose of advising other organizations of potential second order effects resulting from the mission impact. The IIR is the product of the technical assessment details provided by the incident response agent and the most current mission impact assessment provided by the information owner. In nearly all cases, the IIR will be compiled and entered into a consolidated reporting database by the response agent tasked by the NETOPS command and control agency. On Air Force networks, this means that the AFNOC NSD IRT would work directly with the information owner on all IIRs to

ensure the IIR submitted timely and appropriately. The three forms of IIRs are discussed further here.

Initial IIR.

The initial IIR must be submitted in a very timely manner after incident declaration. Air Force NETOPS guidance requires initial incident report submission within one hour after incident declaration. The initial IIR serves to notify the all interested parties in the NETOPS community of an incident on the organization's networks. As previously mentioned, it serves to provide situational awareness to the local organizational decision maker about potential mission impact. However, this situational awareness through impact reporting also alerts the NETOPS command and control and higher command authority of a mission impact incident on the organization's networks. This provides agencies in all directions situational awareness of potential second order effects from potential mission impact at the site of the incident. Additionally, agencies that may have dependencies on the information assets damaged by the cyber incident may elect to perform local defensive cyber damage assessment to determine any immediate impact resulting from the incident that occurred outside of their organization.

As previously stated, the initial IIR contains only limited technical assessment and potential mission impact, based on the potential mission impacted documented in the pre-incident risk assessment activities. The initial IIR provides situational awareness and allows the local organization and agencies throughout the enterprise to posture for potential second order effects that may have been produced by the cyber incident.

Interim IIRs.

In most cases remediation and recovery will begin as early as possible, thus allowing less down time and increased mission continuity. Investigation by the IR function during the incident response stage will facilitate determination of the compromise cause and size.

The interim IIRs are essentially updates that provide more detailed information relating to the cyber incident. The interim IIR is released by the NETOPS ordained IR agent, which on Air Force networks is the AFNOSC NSD. In the first interim IIR the designated IR agent has accomplished some degree of technical investigation and incident response that facilitates more refined damage and mission impact assessment by the information owner. Each subsequent IIR may be an additional refinement, and provide the organization decision maker and all parties of interest a more accurate picture of the actual damage and mission impact that resulted from the cyber incident. Interim IIRs will be issued at set intervals as need or NETOPS authority dictates until the incident is closed.

Final IIRs.

The final IIR is released at the closure of the incident investigation. It signifies that all technical actions, such as investigation, remediation, and recovery, have been completed. It is highly unlikely that new information will become available at this time that is relevant to the information owner's responsibility to determine additional mission impact. The final IIR will contain a full summary of events and technical assessment developed by the IR agent and a final description of the actual mission impact.

Post-incident activities.

The post-incident activities of the CDA-D/MIA framework are important contributors to the continuity of effective CDA-D/MIA operations and cyber security efforts as a whole. The research emphasizes two critical activities that must be achieved following the remediation, recovery, and closure of a cyber incident.

Strategic Accountability Reporting.

Accountability and lesson learned from the incident can have influence on future IT and security planning and investment. Failure to assess the long term impact can hamper efforts to determine such important economic impact factors as, customer confidence, which potentially affects long-term income. From a military perspective, strategic reporting will focus on accountability not only to prevent future occurrences of an information incident, but also assess potential budget impact. The strategic domain of operations is the one place where understanding the cost loss of a cyber incident may be useful to a decision maker.

When a mishap occurs on the flight line, an after actions report is submitted to report the results of how and why the mishap occurred and includes the cost of the mishap in economic terms. The information from these reports are collected and tracked for trends analysis, but are used most importantly for accountability and prevention. For this reason, this research recognizes the need for enterprise post-incident accountability reporting following an incident. Such reporting can reveal trends that may lead to improved security practices and reduction in risk to information assets. Additionally, it can help the Air Force understand the enormous cost of repeated incidents in a time when budgetary constraints force more frugal investment. Most importantly, post-incident

accountability reporting will hold those accountable who disregard security controls or otherwise introduce unnecessary and actualized risk against the critical information assets on which mission operations depend. Strategic post-incident accountability reporting would offer the Air Force enterprise several advantages in understanding and preventing cyber incidents that it currently does not enjoy.

Periodic Asset Valuation.

Events may occur that result in an asset identified as critical to experience reduction in its utility by the organization to such an extent that it may no longer be as important to the organization. Events such as shifts in the organization's mission, lifecycle issues that have caused a the asset to outlive its usefulness, an incident that has irreparably damaged an asset's confidentially value, or bringing a new system online that contains information assets and data stores that replace the existing can all result in permanent devaluation of the information asset. For any of these reasons, it is critical that the organization establish a periodic and scheduled re-visitation of the risk assessment activity. This is not only a good security and risk management practice, but it ensures that all critical assets continue to be identified within the organization and the value documentation in the asset's CIAP is maintained accurately.

Limitations.

All research maintains some limitations despite the best efforts of the researcher. This research effort is no exception. One such limitation was bias. The investigator was motivated to this research by experiences gained while professionally employed in network defense incident response operations. Despite great and sincere efforts to remain

objective, there is a high probability that some degree of investigator bias was introduced by the researcher's experience. Additionally, sample bias imposed limitations on this research effort. The targeted population was limited to 18-20 possible interviewees to ensure the integrity of response data. Most research efforts would prefer a larger sample. This issue was compounded by non-response bias. Since the sample was self-selected through voluntary participation, only 9 personnel elected to participate. This represented only half of the targeted population, and potentially resulted in failure to collect important relevant responds data.

Another limitation of this research was the scope. The problem of damage and mission impact assessment is complex, and consists of many activities with strong interdependencies. Failure to accurately and effectively accomplish one of these activities creates a ripple effect that taints the quality of the systems of activities that comprise cyber damage and mission impact assessment. No study exists that looks at the entire process. Therefore this scope of this research project is large by necessity. This fact limits the ability to examine the components in great detail, as deserving of such an important area of research.

Recommendations.

This research has made of number of recommendations for improvement to the current damage and mission impact assessment methodology by proposing a new methodology to do this. The prevailing theme throughout the research was the need to relax the exclusive focus on technology to allow a more comprehensive understanding of cyber protection and mission impact assessment. The Air Force, and indeed, the DoD

must understand the purposes of network defense is not to protect the network for the network's sake. Rather, its purpose is to protect the information assets on the network. It is the information on the network that allows the bombs to drop on target and allows to commander to make the right decisions in the battlespace.

As the Air Force moves towards standing up a new Cyber Command, it is imperative that information takes center stage in cyber operations. Many sections of private sector industry have been moving in this direction of several years. The Air Force would be wise to understand industry "best practices" will work in the unique environment of military operations. Failure to do so may cause continuation of limitations that currently plague Air Force network operations, and especially defensive cyber damage and mission impact assessment efforts.

Areas for Future Research.

The scope of this research was very high level by necessity. The goal of the research was understand the current state of damage and mission impact assessment in order to propose a methodology offering improvements over the current implementation. It was necessary to abstract many functions, which leaves considerable room for additional research.

Operational Validation.

The proposed methodology is conceptual. To ensure that an operationalized methodology is attainable, the concepts of this proposed CDA-D/MIA methodology most be validated. Ideally, performing the proposed risk assessment activities to identify the assets in a mock operational arena, such as a test Combined Air Operations Center at

Nellis Air Force Base (CAOC-N) would be an ideal scenario to test the proposed methodology and concepts. Both shortcomings and successes of the conceptual methodology would quickly be revealed in all aspects of the methodology, but especially in the damage assessment and mission impact reporting areas.

The recommended approach would be to "artificially" identify a small quantity of assets. By artificial identification, it is meant that the CAOC system, associated information assets on the system, and mission relationships are known quantities and not discovered through risk assessment. Test scenarios may be run against the systems to accurately evaluate the methodology's effectiveness at assessing damage and mission impact; and the quality and accuracy of mission impact reporting.

Automation of Assessment and Reporting.

The conceptual methodology is extremely human labor-intensive. Certainly, an effective methodology can not completely separate itself from human involvement, especially in the areas of risk assessment and asset identification, but there are some aspects that are suitable for automation. Further research into the development of damage and mission impact automation and reporting is recommended. The pre-incident loading activities of asset identification, value determination, and attribute documentation are highly subjective and will very greatly from organization to organization. These activities must necessarily maintain a high human involvement. However, once these values are loaded, the possibilities for automated damage detection and assessment, and subsequent mission impact assessment and reporting, are great. Recommended research in this area is database development that would facilitate asset attribute loading to enable

dynamic asset dependency mappings from system to asset, but also easier mapping of trans-asset dependencies.

Asset Value Models.

This research has proposed a new approach to establishing value handles to the intangible value qualities of information assets. This approach seeks to assess asset value as a function of the relationship the asset holds to the mission, and is based on the constructs established in the proposed conceptual construct model. The value rating scale is intentionally simplistic for the purposes of illustrating how the relative value the asset maintains can be estimated and reflected with minimal complexity of use. However, further research in developing more mature value models is recommended.

Future models should hold true to the concept of value as a reflection of utility, and value assignment as an estimation of the approximate "strength" of this relationship. Development of such a value model may have a profound impact on the assessment of information value in areas beyond military networks.

Asset-Focused Risk Assessment and Asset Identification.

This research found that accurate identification, valuation, and documentation is the foundation for any subsequent damage and mission impact assessment activities. This critical activity is not being accomplished effectively for Air Force cyber information. Further research in improved methodology for information asset identification would be beneficial to only damage and mission impact methodology, but to all aspects of Air Force cyber security. There are many avenues from which to begin such research, but it is important that the research focus on development on a risk identification and assessment methodology that focuses on information as an asset.

Chapter Summary

This chapter proposed conceptual methodology for defensive cyber damage and mission impact assessment. The chapter opened with a discussion of foundational concepts critical to the establishment of such a proposed model. This proposal was the result of the extensive literature review of publications, thorough examination of related research of damage assessment on Air Force networks, and interviews with personnel professional involved with the current damage and mission impact assessment efforts. The purpose of this research is to establish a comprehensive understanding of the state of mission impact assessment on Air Force network in order to propose an improved methodology.

Appendix A

Case Study Interview Questions

SECTION 1: INTERVIEWEE INFORMATION

1. Interviewee #:

2. Are you currently or have you been professionally involved with Network Warfare Operations (NWO) or Network Defense (NetD) activities on Air Force networks? NWO is defined by AFDD 2-5.

SECTION 2: INCIDENT DAMAGE /MISSION IMPACT ASSESSMENT

1. In your experience, does current incident damage assessment methodology on Air Force networks comply with the requirement of *CJCSM 6510.01 Ch 3 Annex A to Appendix B to Enclosure B* prescribing operational impact assessment of a DoD organization affected by a computer security incident?

2. In your experience, how well are responsible Net-D activities (incident response, forensics activities, etc.) able to estimate the impact to an organization's mission capability resulting from and incident on Air Force networks?

3. Based on your response to question #3, what factors, if any, contribute to the level of effectiveness estimating the impact to an organization's mission capability resulting from and incident on Air Force networks?

Appendix B

Information Asset Profile Worksheets

MISSION PROCESS WORKSHEET	CRITICAL INFORMATION ASSET DOCUMENTATION WORKSHEET			
MISSION PROCESS IDENTIFIER (MPID):			CRITICALITY RATING	
DATE			VERSION	
	NAME/OFFICE	CONTACT INFORMATION		
PROCESS OWNER				
PROCESS OWNER				
PROCESS OWNER				
	NAME/OFFICE	CONTACT INFORMATION		
PROFILE AUTHOR				
MISSION PROCESS DESCRIPTION (How does this process support the organization's mission? Is it an essential process? Why?)				
EXPECTED IMPACT TO MISSION FROM PROCESS LOSS				
KNOWN DEPENDENCIES (What other processes rely on this process?)				
ADDITIONAL NOTES				

Figure 25. CIAP Worksheet: Mission Process Worksheet

INFORMATION PROCESS WORKSHEET	CRITICAL INFORMATION ASSET DOCUMENTATION WORKSHEET			
INFORMATION PROCESS IDENTIFIER (IPID):			CRITICALITY RATING	
DOCUMENTATION DATE			DRAFT VERSION	
SUPPORTS:	#1	#2	#3	#4
MPID				
OWNER				
	NAME/OFFICE		CONTACT INFORMATION	
PROCESS OWNER				
PROCESS OWNER				
PROCESS OWNER				
	NAME/OFFICE		CONTACT INFORMATION	
PROFILE AUTHOR				
INFORMATION PROCESS DESCRIPTION (How does this information process support critical mission processes?)				
EXPECTED IMPACT TO SUPPORTED MISSION PROCESS IF LOST				
KNOWN DEPENDENCIES (What other processes rely on this process?)				
ADDITIONAL NOTES				

Figure 26. CIAP Worksheet: Information Process Worksheet

ASSET PROFILE WORKSHEET	CRITICAL INFORMATION ASSET DOCUMENTATION WORKSHEET			
CRITICAL ASSET IDENTIFIER:			CRITICALITY RATING	
DOCUMENTATION DATE			CLASSIFICATION	
SUPPORTS:	#1	#2	#3	#4
INFO PROC ID				
PROC OWNER				
	NAME/OFFICE		CONTACT INFORMATION	
ASSET OWNER				
ASSET OWNER				
	NAME/OFFICE		CONTACT INFORMATION	
ASSET CUSTODIAN				
ASSET CUSTODIAN				
	NAME/OFFICE/AGENCY		CONTACT INFORMATION	
ASSET PRODUCER				
ASSET PRODUCER				
KNOWN TRANS-ORGANIZATIONAL DEPENDENCIES				
	NAME/OFFICE/AGENCY		CONTACT INFORMATION	
ASSET CONSUMER				
ASSET CONSUMER				
ASSET CONSUMER				
ASSET CONSUMER				
GENERAL DESCRIPTION OF CRITICAL ASSET				
CONTAINER	**SYSTEM ID**	**LOCATION**	**CUSTODIAN**	
1				
2				
3				
NOTES AND COMMENTS				
ASSET PROFILER: (Name/Org/Contact)				PAGE 1

Figure 27. CIAP Worksheet: Asset Profile Worksheet – Page 1

ASSET VALUATION WORKSHEET PAGE 2	CRITICAL INFORMATION ASSET DOCUMENTATION WORKSHEET					
CRITICAL ASSET IDENTIFIER				CRITICALITY RATING		
DATE				CLASSIFICATION		
SUPPORTS:	#1	#2	#3	#4		
IPID						
IPID OWNER						
	NAME/OFFICE		CONTACT INFORMATION			
ASSET OWNER						
CONSTRUCT VALUATION						
MISSION BINDING		**IS CRITICAL**	**Value:**			
SUPPORTS MPID:		Y / N				
SUPPORTS IPID:		Y / N				
DESCRIPTION / COMMENTS						
AGE			**Value:**			
TIME CRITICAL	Y / N	**EXPECTED LIFESPAN**				
DESCRIPTION / COMMENTS						
STATE VALUES						
CONFIDENTIALITY			**Value:**			
CRITICAL	Y / N	Comment:				
DESCRIPTION AND COMMENTS						
INTEGRITY			**Value:**			
CRITICAL	Y / N	Comment:				
RESTORABLE?	Y / N	Comment:				
DESCRIPTION AND COMMENTS						
AVAILABILITY			**Value:**			
CRITICAL	Y / N	Comment:				
DESCRIPTION AND COMMENTS						
ASSET PROFILER: (Name/Org/Contact)					PAGE 2	

Figure 28. CIAP Worksheet: Asset Profile Worksheet – Page 2

CONTAINER PROFILE WORKSHEET	CRITICAL INFORMATION ASSET DOCUMENTATION WORKSHEET PG -1						
SYSTEM IDENTIFIER					CRITICALITY RATING		
DOCUMENTATION DATE					SYSTEM CLASSIFICATION		
SUPPORTS:	#1	#2	#3	#4	#5	#6	#7
CRITICAL ASSET IDENTIFIER:							
SYSTEM INFO:	NAME/OFFICE			CONTACT INFORMATION			
SYSTEM OWNER							
SYS ADMIN							
	BUILDING/RM			LOCATION NOTES:			
LOCATION							
	NAME/OFFICE/AGENCY			CONTACT INFORMATION			
OTHER CONTACT:							
OTHER CONTACT:							
APPLICATIONS	MISSION SUPPORT NOTES:						
OPERATING SYSTEM							
CRITICAL SYSTEM APPLICATIONS							
OTHER APPLICATIONS							
HARDWARE	TECHNICAL INFORMATION						
FUNCTIONAL ROLE							
TECHNICAL SPECIFICIATONS							
ASSET PROFILER: (Name/Org/Contact)							PAGE 1

Figure 29. CIAP Worksheet: Container Profile Worksheet - Page 1

CONTAINER PROFILE WORKSHEET	CRITICAL INFORMATION ASSET DOCUMENTATION WORKSHEET- PG 2						
SYSTEM IDENTIFIER					CRITICALITY RATING		
DOCUMENTATION					SYSTEM		
SUPPORTS:	#1	#2	#3	#4	#5	#6	#7
CRITICAL ASSET IDENTIFIER:							
NETWORK	NETWORK NOTES:						
DOMAIN INFORMATION							
DEPENDENCIES							
SUPPORT CONTACTS							
CONTAINER NOTES	CONTAINER NOTES:						
DEPENDENCIES ON OTHER CONTAINER							
SPECIAL CONSIDERATIONS:							
CONTINUATION NOTES:							
ASSET PROFILER: (Name/Org/Contact)							PAGE 2

Figure 30. CIAP Worksheet: Container Profile Worksheet - Page 2

Bibliography

AFDD 2-5 (2005). Air Force Doctrine Document (AFDD) 2-5 Information Operations. Department of the Air Force, HQ AFDC/DR: pp.80.

AFI 10-206 (2004). Air Force Instruction (AFI) 10-206: Operational Reporting. Department of the Air Force, HQ USAF/XO: pp.87.

AFI 33-138 (2004). Air Force Instruction (AFI) 33-138: Enterprise Network Operations Notification and Tracking. Department of the Air Force, SAF/XCIF**:** pp. 81.

AFI 51-4 (1993). Air Force Policy Directive (AFPD) 51-4: Compliance with the Law of Armed Conflict. Department of the Air Force, HQ USAF/JA: pp. 4.

AFI 51-402 (1994). Air Force Instruction (AFI) 51-402: Weapons Review. Department of the Air Force, HQ USAF/JAI: pp.3.

AFI 90-901 (2001). Air Force Instruction (AFI) 90-901: Operational Risk Management. Department of the Air Force, HQ USAF/SEP: pp.77.

AFPD 90-9 (2000). Air Force Policy Directive (AFPD) 90-9: Operational Risk Management. Department of the Air Force, HQ USAF/SE: pp.5.

Alavi, M. and D. E. Leidner (1999). "Knowledge management systems: issues, challenges, and benefits". Communications of the Association for Information Systems 7(1).

Alberts, C. J. and Dorofee, A. (2001*)."* Appendix D: Overview of the OCTAVE Method*"*. *OCTAVE Method Implementation Guide Version 2.0*. Pittsburg PA, Carnegie Mellon University.

Alberts, C. J. and Dorofee, A. (2005). "Mission assurance analysis protocol (MAAP): assessing risk in complex environments". Networked Systems Survivability Program, Pittsburgh PA, Carnegie Mellon University: pp.50.

Alberts, C. J., A. Dorofee, et Al. (2003). “Introduction to the OCTAVE approach”. Pittsburgh PA, Carnegie Mellon University: pp.37.

Alberts, D. S. (1996). Defensive information warfare. Washington D.C., National Defense University Press.

Allard, C. K. (1990). Command, control, and the common defense. New Haven, CT, Yale University Press.

American Heritage (n.d.,). "cyberspace". The American Heritage New Dictionary of Cultural Literacy, Third Edition. Retrieved December 27, 2006, from http://dictionary.reference.com/browse/cyberspace.

Arquilla, J. and Ronfeldt, D. (1993b). Cyberwar is Coming! in In Athena's camp: preparing for conflict in the Information Age. eds J. Arquilla and D. Ronfeldt. Santa Monica CA, RAND**:** pp.23-60.

Arvidsson, J. (n.d.). "Taxonomy of the Computer Security Incident Related Terminology". Retrieved 11 June 2006, from http://www.terena.org/activities/tf-csirt/iodef/docs/i-taxonomy_terms.html.

Baskerville, R. L. and Im. G. P. (2005). "A longitudinal study of information system threat categories: the enduring problem of human error". Database for Advances in Information Systems. 36(4): pp.68-79.

Billo, C. and Chang, W. (2004). Cyber warfare: an analysis of the means and motivations of selected nation states. Hanover NH, Institute for Security and Technical Studies at Dartmouth College.

Bishop, M. (2003). Computer security: art and science. Boston MA, Addison-Wesley.

Blodgett, M. (1999). "Is your business as safe as you think?" Retrieved December 24, 2006, from http://www.cnn.com/TECH/computing/9907/16/security-ent.idg/.

Bowman, E. H. and Moskowitz, G. T. (2001). "Real options analysis and strategic decision making". Organization Science 12(6): pp.772-777.

Boyd, J. R. (1996). "The Essence of Winning & Losing: Boyd's Last Briefing". Retrieved January 2, 2007, from http://www.belisarius.com/modern_business_strategy/boyd/essence/eowl_frameset.htm.

Bragg, R. (2002). “Risk Management and Analysis”. in Certified Information Systems Security Professional Training Guide (electronic version). Indianapolis IN, Que. Retrieved August 23, 2006, from http://www.informit.com/articles/article.asp?p=30287&seqNum=4&rl=1

Buffett, S. F., Scott, N., Richter, M.M, Spencer, B. (2004). Determining internet users' values for private information. Conference on Privacy, Security and Trust (PST'04), New Brunswick, Canada, National Research Council Canada.

Bush, G. H. W. (1990). National Security Directive No. 42 (NSD-42): National Policy for the Security of National Telecommunications and Information Systems. White House. Washington, D.C.

Bush, G. W. (2003). "Homeland Security Presidential Directive No. 7 (HSPD-7)". Retrieved December 12, 2006, from http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

Bush, G. W. (2004). “President's Radio Address to the Nation on July 24, 2001”. Retrieved October 22, 2006, from http://www.whitehouse.gov/news/releases/2004/07/20040724.html

Butts, J. W. (2006). “Formalizing the insider threat through security modeling and risk analysis”. Department of Electrical and Computer Engineering. Wright Patterson Air Force Base, Air Force Institute of Technology: pp.92.

Carr, N. G. (2003). "IT doesn't matter " Harvard Business Review. 81(5): pp. 41-49.

CERT. (2006). "Statistics 1988-2006: Incidents Reported". Retrieved 11 May, 2006, from http://www.cert.org/stats/cert_stats.html.

Charron, M. P. (1987). "Risk Identification". Journal of Property Management 52(2): pp.80-83.

Chinchani, R., Iyer, A. et Al. (2005). “Towards a theory of insider threat assessment”. Proceedings of the International Convergence on Dependable Systems and Networks, Yokohama Japan: pp.108-117.

CJCSM6510.01 (2006). Chairman of the Joint Chiefs of Staff Manual No. 6510.01 Ch3 Annex A to Appendix B to Enclosure B, all changes as of 08 March 2006, Chairman Joint Chief of Staff: pp.118.

Clarke, R. (2003). “Interview for PBS Frontline: Cyber War!” Retrieved November 12, 2006, from http://www.pbs.org/wghb/pages/frontline//shows/cyberwar/interviews/clarke.html

Computer Desktop Encyclopedia (n.d.). "information owner." Computer Desktop Encyclopedia. Retrieved January 09, 2007, from http://www.answers.com/topic/information-owner.

Curry, H. (2004). "The current battle damage assessment paradigm is obsolete". Air & Space Power Journal 18(4): pp.13-17.

Davenport, T. H. and Prusack, L. (1998). Working Knowledge: How Organizations Manage What They Know. Boston MA, Harvard Business School Press.

Denning, D. (1999). Information warfare and security. Upper Saddle River NJ, Pearson.

Denning, D. (2001). “Activism, 'hacktivisim', and cyberterrorism: the Internet as a tool for influencing foreign policy”. in Networks And Netwars: The Future Of Terror, Crime, And Militancy. eds J. Aquilla and D. Ronfeldt. Santa Monica CA, RAND: pp.239-288.

DiCenso, D. J. (1999). "IW Cyberlaw: the legal issues of information warfare". Aerospace Power Journal 13(2): pp.85-102.

DiDio, L. (1998) "U.S. Coast Guard beefs up security after hack." Computerworld". Retrieved September 03, 2006, from http://www.cnn.com/TECH/computing/9807/22/coastguard.idg/

Diehl, J. G. and Sloan, C. E. (2005). "Battle damage assessment: the ground truth". Joint Force Quarterly. 37(1): pp.59-64.

DOD (1992). Final Report to Congress: Conduct of the Persian Gulf War, 1992. Washington DC, United States Department of Defense: pp.909.

DODD5220.22-M (2006). *Department of Defense Directive 5220.22-M, National Industrial Security Program Operating Manual*.

Donahue, W. A. (1997). "Statement of Lieutenant General William A. Donahue, Deputy Chief of Staff for Communications and Information, Headquarters, United States Air Force". House Military Procurement and Research and Development Subcommittees. Washington, DC.

Drucker, P. E. (1993). Post-Capitalist Society. New York, Harper Collins.

Drucker, P. E. (1995). Managing In A Time Of Great Change. New York, Penguin.

Dubendorfer, T., Plattner, B., Wagner, A. (2004). "An economic damage model for large-scale internet attacks". IEEE.

Dynes, S., Andrijcic, E., et Al. (2006). "Costs to the U.S. Economy of Information Infrastructure Failures: Estimates from Field Studies and Economic Data". Fifth Workshop on the Economics of Information Security (WEIS 2006). Cambridge U.K., Robinson College, University of Cambridge.

EO13292 (2003). Executive Order 13292 - Further Amendment to Executive Order 12958, as Amended, Classified National Security Information:pp.22.

FAS. (1997). "Air Force Computer Emergency Response Team". Retrieved January 3, 2007, from http://www.fas.org/irp/agency/aia/cyberspokesman/97aug/afcert.htm.

GAO (2000). Federal Information Technology Security Assessment Framework. Washington, D.C., United States Security, Privacy, and Critical Infrastructure Committee: National Institute of Standards and Technology Computer Security Division**:** pp.24.

GAO (2005). "Weaknesses persist at federal agencies despite progress made in implementing related statutory requirements". Information Security. Washington, D.C., United States Government Accountability Office**:** 54.

Gibson, W. (1984). Neuromancer. New York, Ace.

Gordon, L. A., Loeb, M. P., Lucyshyn, W, Richardson, R. (2006). “CSI/FBI Computer Crime and Security Survey”, Computer Security Institute**:** pp.26.

Graham, B. and Eggen, D. (2005) "Hackers Attack Via Chinese Web Sites: U.S. Agencies' Networks Are Among Targets”. The Washington Post[Online] Retrieved November 12, 2006, from: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318_pf.html

Grance, T., Kent, K. et Al. (2004). “Computer Security Incident Handling Guide”. NIST SP 800-61. Gaithersburg MD, National Institute of Standards and Technology**:** pp.148.

Green, J. (2002). "The Myth of Cyberterrorism: There are many ways terrorists can kill you--computers aren't one of them”. Washington Monthly. Retrieved November 12, 2006, from http://www.washingtonmonthly.com/features/2001/0211.green.html.

Grimes, J. G. (n.d.). "Welcome statement of Hon. John G. Grimes, Assistant Secretary of Defense (Networks & Information Integration) and DoD CIO”. Retrieved January 30, 2006, from http://www.dod.mil/cio-nii/.

Gruber, D. J. (2000). “Computer networks and information warfare: implications for military operations”. Maxwell Air Force Base, AL, Center for Strategy and Technology, Air War College, Air University.

Gumahad, A. T. (1997). "Cyber troops and net war: the profession of arms in the information age”. Joint Force Quarterly. (Spring): pp.14-20.

Hampton, J. J. (2006). "Emerging risk strategies”. Business Insurance 40(36): p.33.

Horony, M. D. (1999). “Information System Incidents: The Development Of A Damage Assessment Model”. Department of Engineering and Management. Wright Patterson Air Force Base, OH, Air Force Institute of Technology.

Howard, J., Longstaff, T. (1998). A Common Language For Computer Security Incidents, Sandia National Labratories.

IEEE-USA. (2006). "Position paper: Cyber security research & development". Retrieved December 27, 2006, from http://www.ieeeusa.org/policy/positions/cybersecurity.asp.

Jackson, W. (2006). "Weak spots on cyberdefense: Interview with O Sami Saydjari, CEO of the Cyber Defense Agency". Government Computer News. (25): p.20.

Jensen, W. P. (2005). Toward Omniscient Command: How to Lead in the Information Age. Fort Leavenworth, KS, School of Advanced Military Studies, United States Army Command and General Staff College.

JP 1-02 (2006). Joint Publication (JP) 1-02: Department Of Defense Dictionary Of Military And Associated Terms, United States Department of Defense.

JP 3-13 (2006). Joint Publication (JP) 3-13: Information Operations. United States Department of Defense.

Kanter, J. (1999). "Knowledge management, practically speaking". Information Systems Management (Fall): pp.7-15.

Kemmerer, R. A. (2003). "Cybersecurity". International Conference on Software Engineering (25th), Portland OR, IEEE Computer Society: pp.705-715.

Kloman, H. F. (1990). "Risk management agonists". Risk Analysis 10(2): pp.201-205.

Kumagai, J. (2003). "The Web as a weapon: cyber warfare". IEEE Spectrum 38(1): pp.118-121.

Lacity, M. C. and M. A. Janson (1994). "Understanding qualitative data: a framework of text analysis methods". Journal of Management Information Systems 11(2): pp.137-155.

Lala, C. and Panda, B. (2000). "Evaluating damage from cyber attacks". IEEE Transactions on Systems, Man and Cybernetics 31(4): pp.300-310.

Leedy, P. D. and J. E. Ormrod (2005). Practical Research Planning and Design. Upper Saddle River NJ, Pearson Prentice Hall.

Lewis, J. (2003, February 18). "Interview for *PBS Frontline: Cyberwar*". Retrieved December 22, 2006, from http://www.pbs.org/wgbh/pages/frontline//shows/cyberwar/interviews/lewis.html.

Lichtenberg, G. (1775). "Notebook D". Retrieved 15 September, 2006, from http://en.wikiquote.org/wiki/Georg_Christoph_Lichtenberg#Quotes_about_Lichtenberg.

Mandia, K., Prosise, C., Pepe, M. (2003). Incident response and computer forensics. Emeryville CA, McGraw Hill/Osborne.

Mark, R. (2005) "Hacker Hits Air Force Officer Database". Internetnews.com. Retrieved 19 September, 2006, from http://www.internetnews.com/security/article.php/3529046

Masterson, M. J. (2004) "Using assessment to achieve predictive battlespace awareness". Air & Space Power Journal [Online]. Retrieved 12 September, 2006, from http://www.airpower.maxwell.af.mil/airchronicles/cc/masterson.html

Mimoso, M. S. (2005, December 22, 2005). "PING with Marcus Sachs". Information Security Magazine [Online]. Retrieved December 12, 2006, from http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1154027,00.html?bucket=ETA&topic=303585.

Morrision, C. T. and Cohen, P. R. (2005). "Noisy information value in utility-based decision making". Proceedings of the 1st international workshop on Utility-based data mining Chicago, Illinois ACM Press.

Moteff, J. (2004). "Computer security: a summary of selected federal law", Washington DC, Congressional Research Service.

NCSC (1988). "Glossary of computer security terms". Fort Meade MD, National Computer Security Center. Retrieved December 13, 2006, from http://packetstormsecurity.org/docs/rainbow-books/NCSC-TG-004.txt

NIAC. (2002). "The National Strategy to Secure Cyberspace". Retrieved November 3, 2006, from http://www.whitehouse.gov/pcipb/.

NIST (1996). “Special Publication 800-12 An introduction to computer security: The NIST handbook”. NIST SP 800-12. Gaithersburg MD, National Institute of Standards and Technology (NIST).

Norman, D. A. (1983). "Design rules based on analyses of human error”. Communications of the ACM 26(4): pp.254-258.

NSA. (n.d.). "The GIG Vision Enabled by Information Assurance”. National Security Agency. Retrieved December 30, 2006, from http://www.nsa.gov/ia/industry/gig.cfm?MenuID=10.3.2.2.

Oxford. (1986). The Oxford Reference Dictionary”. Oxford University Press.

PCD (2002a). “Letter to President Bush”. Professionals for Cyber Defense. Washington DC. Retrieved December 30, 2006, from http://www.uspcd.org/letter.html

PCD. (2002b). "Professionals for Cyber Defense Members”. Professionals for Cyber Defense. Washington DC. Retrieved January 1, 2007, from http://www.uspcd.org/members.html.

Petrocelli, T. D. (2005). Data protection and information lifecycle management. Upper Saddle River NJ, Pearson Education, Inc.

Rezmierski, V., Deering, M. et Al. (1999). Incident cost analysis and modeling project (ICAMP): A report from the CIC security working group to the CIC Chief Information Officers, University of Michigan**:** pp**.**161.

Roberts, C. M. (2004). The Dissertation Journey: A Practical and Comprehensive Guide to Planning, Writing, and Defending Your Dissertation. Thousand Oaks CA, Corwin Press.

Rosencrance, L. (2001) "Teen charged with hacking into Air Force system”. CNN.com . Retrieved December 30, 2006, from http://archives.cnn.com/2001/TECH/internet/04/24/air.force.hack.idg/index.html

Rowe, N. C. (2005). “Ethics of cyberwar attacks”. in Encyclopedia of Cyber War and Cyber Terrorism [Online]. A. Colarik and L. Janczewski. Hershey PA, The Idea

Group. Retrieved August 19, 2006, from http://www.cs.nps.navy.mil/people/faculty/rowe/attackethics.htm

SANS. (2006). "Glossary of Terms Used in Security and Intrusion Detection". Retrieved 31 December, 2006, from http://www.sans.org/resources/glossary.php?portal=2046f43b7629684aa3ac3cf61fd1c1c5#t.

Saydjari, O. S. (2002). "Defending cyberspace". Computer. 35(12): pp.125-127.

Shimeall, T., Williams, P., et Al. (2002). "Countering cyber war". NATO Review. (Winter): pp.16-18.

Shirey, R. (2000). "RFC 2828: Internet Security Glossary". Retrieved December 7, 2006, from http://portalparts.acm.org/rfc_fulltext/fyi/fyi36/fyi36.txt.

Soo Hoo, K. J. (2000). "How Much Is Enough? A Risk Management Approach to Computer Security". Consortium for Research on Information Security and Policy (CRISP), Stanford University **:**pp. 99.

Sopko, M. G. (1999) "Combat assessment: analyzing the results of an air campaign". Air & Space Power Journal. Retrieved December 17, 2006, from http://www.airpower.maxwell.af.mil/airchronicles/cc/sopko.html

Spears, J. L. (2006). The effects of user participation in identifying information security risk in business processes. Special Interest Group on Computer Personnel Research Annual Conference, Claremont CA, ACM Press.

Spiegler, I. (2000). "Knowledge management: a new idea or a recycled concept?" Communications of the Association for Information Systems 3(6):pp. 20.

Stevens, J. F. (2005). *Information asset profiling*. Pittsburgh, PA, Carnegie Mellon University: pp 61.

Stevens, M. M. (2001). "Selected qualitative methods". Interactive Textbook on Clinical Research. M. B. Max and J. Lynn, National Institute of Dental and Craniofacial Research, National Institutes of Health.

Stoneburner, G., Goguen, A., et Al. (2002). “Risk Management Guide for Information Technology Systems”. NIST SP 800-30. Gaithersburg MD, National Institute of Standards and Technology.

Strauss, A. L. and J. Corbin (1990). Basics of Qualitative Research. Newbury Park CA, Sage.

Suellentrop, C. (2006) "Sim City: Terrortown”. Wired. Retrieved September 27, 2006 from http://www.wired.com/wired/archive/14.10/posts.html?pg=2..

Sun-Tzu (1993). Sun tzu : the new translation (the art of war). New York, William Morrow.

Thiem, L. (2005). “A study to determine damage assessment methods or models on Air Force networks”. Department of Engineering and Management. Wright Patterson Air Force Base OH, Air Force Institute of Technology.

Tiboni, F. (2005a). "Army rebuilds network defenses after hacks”. Federal Computer Week [Online]. Retrieved December 27, 2006 from http://www.fcw.com/article89175-06-13-05-Print.

Tiboni, F. (2005b) "The new Trojan war: Defense Department finds its networks under attack from China”. Federal Computer Week [Online]. Retrieved December 27, 2006 from http://www.fcw.com/article90262-08-22-05-Print.

United States Congress (2002). P.L. 107-347 Title III - Federal Information Security Management Act of 2002 (FISMA). United States Congress, Public Law 107-347 - E-Government Act.

USCERT. (2003). "Ridge creates new division to combat cyber threats”. Retrieved June 22, 2006, from http://www.us-cert.gov/press_room/ncsd-announced.html.

Vail, E. F. (1999). "Knowledge Mapping: getting started with knowledge management”. Information Systems Management. (Fall): pp.16-23.

Van Alstyne, M. V. (1999). A proposal for valuing information and instrumental goods. Proceeding of the 20th international conference on Information Systems

Charlotte, North Carolina, United States Association for Information Systems: pp.328-345.

Vatis, M. (2002). Cyber Attacks: Protecting America's Security Against Digital Threats, John F. Kennedy School of Government, Harvard University.

Warden, J. A. (1988). "Defensive Operations". In The Air Campaign[Online]. Washington DC, National Defense University Press. Retrieved November 14, 2006, from http://www.au.af.mil/au/awc/awcgate/warden/warden-all.htm#chapter4

Wesner, J. W., Hiatt, J. M., Trimble, D. C. (1995). Winning With Quality: Apply Quality Principles in Product Development. Boston MA, Addison Wesley Longman.

Whitman, M. E. and Mattord, H.J. (2004). Management of information security. Boston MA, Thompson Course Technology.

Willcocks, L. P. (2004). "Evaluating the outcomes of information systems plans: Managing information technology evaluation - techniques and processes". Strategic Information Management: Challenges and Strategies in Managing Information Systems. R. D. Galliers and D. E. Leidner. Burlington MA, Elsevier Butterworth-Heinemann: pp.239-258.

Wingfield, T. C. (2006). When Is a Cyber Attack an "Armed Attack?": Legal Thresholds for Distinguishing Military Activities in Cyberspace. Arlington VA, Potomac Institute for Policy Studies.

Winkler, I. (2005). Spies Among Us. Indianapolis IN, Wiley Publishing, Inc.

Winkler, J. R., O'Shea, C. J., Stokrp, M.C. (1996). "Information warfare, INFOSEC, and dynamic information defense". in Proceedings of the National Information Systems Security Conference.

Yin, R., K. (2002). Case study research: design and methods. Thousand Oaks CA, Sage Publications.

Vita

Captain Larry W. Fortson, Jr. enlisted in the United States Air Force in 1993. While stationed at RAF Croughton, England, he completed his undergraduate studies at the University of Maryland, European Division where he graduated with a Bachelor of Science degree with high honors in Computer and Information Science. He received his commission through Air Force Officer's Training School, Maxwell Air Force Base, Alabama.

His first assignment was at Lackland Air Force Base, Texas. While there, he worked as an operations crew commander at the 33d Information Operations Squadron, Air Force Network Operations Center Network Security Division. He deployed to Baghdad, Iraq where he stood up the first operational Information Assurance and Cyber Incident Response Cell. As the cell Chief, he was directly responsible for handling cyber security issues on Multinational Forces – Iraq/Multinational Corps-Iraq warfighting networks. His post-graduation assignment is to Air Force Research Laboratories, Wright Patterson Air Force Base, Ohio.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
22-03-2007	Master's Thesis	Aug 2005 – Mar 2007

4. TITLE AND SUBTITLE

Towards The Development Of A Defensive Cyber Damage And Mission Impact Methodology

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Fortson, Larry W. Fortson, Jr.

5d. PROJECT NUMBER
O7-376

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/07-M9

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFRL/HEX
Attn: Capt Lisa S. Thiem
2255 H Street Bldg 248
Wright Patterson AFB, OH 45433 DSN: 674-5736

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research is to establish a conceptual methodological framework that will facilitate effective cyber damage and mission impact assessment and reporting following a cyber-based information incidents. Joint and service guidance requires mission impact reporting, but current efforts to implement such reporting have proven ineffective. This research seeks to understand the impediments existing in the current implementation and to propose an improved methodology. The research employed a hybrid historical analysis and case study methodology for data collection through extensive literature review, examination of existing case study research and interviews with Air Force members and civilian personnel employed as experts in cyber damage and mission impact assessment of Air Force networks. Nine respondents provided valuable first hand information about the current implementation cyber damage and mission impact assessment. This research identified several critical impediments to current mission impact assessment efforts on Air Force networks. Based upon these findings, a proposal is made for a new operations-focused defensive cyber damage and mission impact methodology. The methodology will address the critical impediments identified and will result in profound benefits in other areas of cyber asset protection. Recommendations for conceptual implementation and operationalization are presented and related future research topics are discussed.

15. SUBJECT TERMS
Information Warfare, Information Security, Risk Management, Damage Assessment, Impact Assessment, Information Asset, Information Value

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			**Michael R. Grimaila, PhD**
U	**U**	**U**	**UU**	254	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 4800; Michael.Grimaila@afit.edu